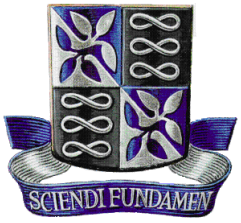
Universidade Federal da Bahia
Instituto de Matemática
Programa de Pós-Graduação em Matemática
Dissertação de Mestrado



Limitação inferior para o grau de comutatividade de um p-grupo de classe maximal

Moacyr Rodrigues de Miranda Júnior

Salvador-BA
Março de 2015

Limitação inferior para o grau de comutatividade de um p-grupo de classe maximal

Moacyr Rodrigues de Miranda Júnior

Dissertação de Mestrado apresentada ao Colegiado da Pós-Graduação em Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do Título de Mestre em Matemática.

Orientadora: **Profa. Dra. Carmela Sica**

Salvador-BA
Março de 2015

À minha família e meus amigos: são tudo pra mim!

Agradecimentos

Agradeço a Deus pelas graças alcançadas a cada dia. Agradeço à minha avó Lygia, a meu "Avohai" Nelson, à minha mãe Elisa Emília, a meus irmãos Manoel Joaquim, Bárbara Mônica e Ana Paula, meu primos Antônio Joaquim e Emília, e à minha namorada Lis Helena, pelo apoio, companherismo, incentivo, conselhos e amor de uma família. Agradeço também aos meu colegas e amigos de todos os "setores" da vida pelo apoio e carinho de sempre. Por contribuir diretamente na realização deste trabalho, agradeço muito e explicitamente à minha colega e amiga Ana Carolina. Agradeço aos professores, que tanto ajudaram na minha formação acadêmica e pessoal, tanto da graduação quanto do mestrado. Em especial, faço um agradecimento ao Professor Mauricio Sicre, meu orientador na graduação, assim como agradeço à fantástica Professora Carmela Sica, minha orientadora nesta dissertação, por toda atenção, cuidado, paciência, compreensão e ajuda tamanha. Ainda, agradeço ao Professor Ciro Russo pela atenção e amizade construída. Agradeço também aos professores da banca examinadora pela atenção e cuidado com as sugestões.

"(...)Pra cada pecado sempre existe um perdão. Não tem certo nem errado: todo mundo tem razão, e (que) o ponto de vista é que é o ponto da questão".

Raul Seixas

Resumo

Seja c a classe de nilpotência do grupo G. É fácil observar que, se a ordem do grupo G é p^m, o número c é sempre menor ou igual a $m-1$. Um p-grupo finito se chama de classe maximal se sua classe é igual a $m-1$. Nos p-grupos de classe maximal é possível definir uma série $G = G_0 > G_1 > G_2 > G_3 > .... > G_{m-1} = 1$, onde G_1 é o centralizador em G de $\gamma_2(G)/\gamma_4(G)$ e $G_i = \gamma_i(G)$, para $i \geq 2$; como de costume $\gamma_i(G)$ é o i-ésimo termo da série central inferior. Definimos o grau de comutatividade de G por $l(G) = \max\{k \mid [G_i, G_j] \leq G_{i+j+k}, i \geq 1, j \geq 1\}$. Este trabalho será sobre a pesquisa de uma limitação inferior para $l(G)$ em função de m e do primo p, e mostrará dois resultados: o primeiro, devido a Leedham-Green e McKay, e o segundo, atribuído a Fernández-Alcober.

Palavras-chave: p-grupos finitos; p-grupos de classe maximal; grau de comutatividade.

Abstract

Let c be the nilpotency class of the group G. It is easy to see that if the order of the group G is p^m, the number c is always less than or equal to $m-1$. A finite p-group is called of maximal class if its nilpotency class is equal to $m-1$. For p-groups of maximal class it is possible to define a series $G = G_0 > G_1 > G_2 > G_3 > .... > G_{m-1} = 1$, where G_1 is the centralizer in G of $\gamma_2(G)/\gamma_4(G)$ and $G_i = \gamma_i(G)$, for $i \geq 2$; as usual, $\gamma_i(G)$ is the i-th term of the lower central series. We define the degree of commutativity of G by $l(G) = \max\{k \mid [G_i, G_j] \leq G_{i+j+k}, i \geq 1, j \geq 1\}$. Our aim is looking for a lower bound for $l(G)$ in terms of m and the prime p, and showing two results: the first one, due to Leedham-Green and McKay, and the second one, due to Fernández-Alcober.

Keywords: finite p-groups; p-groups of maximal class; degree of commutativity.

Sumário

Introdução

Em 1958 foi introduzido por N. Blackburn um dos invariantes mais importantes relacionados a p-grupos de classe maximal: o grau de comutatividade $l(G)$. O grau de comutatividade é uma medida de quão próximo de ser comutativo é um subgrupo G_i, que corresponde a termos da chamada Série Central Inferior de G, para $i \geq 2$. G_1 é o chamado *primeiro Centralizador de Dois Passos*. De acordo com o grau de comutatividade, podemos obter informações a respeito da estrutura do grupo G, como, por exemplo, se a ordem do grupo G é p^m, com p um número primo, então $l(G) = m - 2$ se, e somente se, G_1 é abeliano. Blackburn conseguiu alguns resultados a respeito dos termos da Série Central Inferior do grupo G para $p = 3$ e $p = 5$. C. R. Leedham-Green e S. McKay generalizaram os resultados obtidos por Blackburn, para primos arbitrários. Leedham-Green e McKay mostraram que a limitação $2l(G) \geq m - 3p + 6$ vale para qualquer p-grupo de classe maximal. Posteriormente, G. A. Fernández-Alcober melhorou a limitação de Leedham-Green e McKay, para todo primo $p \geq 7$, sendo a nova limitação $2l(G) \geq m - 2p + 5$. Essa última limitação não contempla os primos $p = 2$, $p = 3$ e $p = 5$, que têm suas limitações do grau de comutatividade verificadas separadas. Neste trabalho, vamos apresentar, além das ferramentas básicas da teoria utilizada na construção das limitações, a demonstração da limitação obtida por Leedham-Green e McKay, e, como objetivo principal do trabalho, a obtida por Fernández-Alcober.

Esta dissertação está organizada da seguinte forma:
No capítulo 1, apresentaremos a definição, caracterizações e alguns resultados relevantes a respeito dos grupos nilpotentes.
No capítulo 2, vamos apresentar os p-grupos finitos e alguns resultados importantes, os p-grupos regulares e alguns resultados que servirão de ferramentas na demostração do resultado principal deste trabalho, além de definirmos e discutirmos a importância do estudo do grau de comutatividade de um p-grupo de classe maximal. Apresentaremos ainda o conceito de elementos uniformes, a cadeia construída a partir de tais elementos, e a função α associada a essa cadeia, e a demonstração da validade de suas propriedades. A função α pode ser considerada a ferramenta-chave na obtenção do resultado objetivado por este trabalho.

No capítulo 3, apresentaremos alguns lemas e o Teorema devido a Leedham-Green e Mckay, o qual apresenta uma limitação inferior para o grau de comutatividade.
Finalmente, no capítulo 4, vamos apresentar alguns lemas e o resultado principal desse estudo, que é o teorema atribuído a Fernández-Alcober, teorema esse que é uma melhoria da limitação inferior do grau de comutatividade $l(G)$ obtida por Leedham-Green e McKay.

Capítulo 1

Algumas definições e resultados básicos

1.1 Grupos nilpotentes

Definição 1.1.1. *Dizemos que um grupo G é* ***nilpotente de classe*** *c se existe uma série de subgrupos (que é chamada série central) $1 = H_0 \leq H_1 \leq ... \leq H_c = G$, onde cada $H_i \trianglelefteq G$ e $\frac{H_i}{H_{i-1}} \leq Z\left(\frac{G}{H_{i-1}}\right)$. A classe de nilpotência c é definida como o menor comprimento de uma série central, e denotada por $cl(G)$.*

Podemos caracterizar um grupo nilpotente através de algumas séries centrais particulares. Apresentaremos a seguir as séries centrais superior e inferior, dadas para um grupo G qualquer. Posteriormente, veremos condições de caracterização dos grupos nilpotentes através de tais séries.

Definição 1.1.2. *É chamada* ***série central superior*** *a série crescente*

$1 = Z_0(G) \leq Z_1(G) = Z(G) \leq \cdots \leq Z_i(G) \leq \cdots$, *onde* $Z_0(G) = 1$ *e* $\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right)$.
Veremos a seguir, através de um resultado, que o grupo G é nilpotente de classe c se, e somente se, a série central superior é da seguinte forma:
$1 = Z_0(G) < Z_1(G) = Z(G) < \cdots < Z_{c-1}(G) < Z_c(G) = G$.

Definição 1.1.3. *Sejam x, y e z elementos de um grupo G. Definimos o* ***comutador de*** *x* ***e*** *y por $[x, y] = x^{-1}y^{-1}xy$. Além disso, convencionamos a escrita $[x, y, z] = [[x, y], z]$. Se H e K são subgrupos de G, denotamos por $[H, K] := \langle [h, k], h \in H, k \in K \rangle$ o subgrupo comutador.*

O resultado a seguir nos fornece algumas propriedades de operação dos comutadores de elementos x, y e z de um grupo G.

Lema 1.1.4. *Sejam x, y e z elementos de um grupo G, e $H, K \leq G$. Então:*

(i) $[x, y] = [y, x]^{-1}$;

(ii) $[xy,z] = [x,z]^y[y,z]$ *e* $[x,yz] = [x,z][x,y]^z$;

(iii) $[x,y^{-1}] = ([x,y]^{y^{-1}})^{-1}$ *e* $[x^{-1},y] = ([x,y]^{x^{-1}})^{-1}$;

(iv) $[x,y^{-1},z]^y.[y,z^{-1},x]^z.[z,x^{-1},y]^x = 1$ *(Identidade de Hall-Witt);*

(v) Se N é um subgrupo normal de G, então $[HN/N, KN/N] = [H,K]N/N$.

A prova do lema acima pode ser encontrada em [5], pg. 123.

Teorema 1.1.5 (Lema dos três subgrupos)**.** *Sejam H, K e L subgrupos de G, e seja N um subgrupo normal de G. Se* $[H,K,L] \leq N$, $[K,L,H] \leq N$, *então* $[L,H,K] \leq N$.

Demonstração. Vamos demonstrar usando o quociente G/N. Nesse caso, N é trivial. Daí, por hipótese, $[H,K,L] = [K,L,H] = 1$, ou seja, $[h,k,l] = [k,l,h] = 1$, $\forall\ h \in H$, $k \in K$ e $l \in L$. Ainda, temos $[h,k^{-1},l]^k = [k,l^{-1},h]^l = 1$. Pela Identidade de Hall-Witt, $[l,h^{-1},k] = 1$, $\forall\ h \in H$, $k \in K$ e $l \in L$. Portanto, $[L,H,K] = 1$, isto é, é trivial no quociente. □

Definição 1.1.6. *Seja X um subconjunto não-vazio do grupo G. O fecho normal de X em G é a interseção de todos os subgrupos normais de G que contêm X. Esse subconjunto de G é um subgrupo normal de G e é denotado por* X^G.

Proposição 1.1.7. *Se* $G = \langle X \rangle$, *então* $G' = \langle [x,y] \mid x,y \in X \rangle^G$

Demonstração. Seja $T = \langle [x,y], x,y \in X \rangle^G$, como G/T é abeliano, pois os geradores comutam, temos que $G' \leq T$. Como $T \leq G'$, temos a igualdade. □

Podemos definir também a série central inferior de um grupo G, cujos termos são de grande importância para o estudo em questão.

Definição 1.1.8. *Definimos indutivamente* $\gamma_1(G) = G$ *e* $\gamma_{i+1}(G) = [\gamma_i(G), G]$, *onde* $[\gamma_i(G), G]$ *é o subgrupo comutador. Como* $\gamma_{i+1}(G) \leq \gamma_i(G)$, *esses subgrupos formam uma série decrescente chamada* ***série central inferior*** *do grupo G. Mostraremos a seguir que o grupo G é nilpotente de classe c se, e somente se,* $\gamma_{c+1}(G) = 1$, *ou seja, a série central inferior é*

$G = \gamma_1(G) > \gamma_2(G) > ... > \gamma_{c+1}(G) = 1$.

Sendo c a classe de nilpotência do grupo G, temos que, se a ordem do grupo G é p^m, o número c é sempre menor ou igual a $m-1$, como veremos posteriormente.

Vamos apresentar agora alguns resultados a respeito dos termos das séries centrais.

Proposição 1.1.9. *Seja G um grupo nilpotente, e seja* $1 = H_0 \leq H_1 \leq \cdots \leq H_n = G$ *uma série central de G. Então* $[H_{i+1}, G] \leq H_i$, $\forall\ i \geq 1$.

Demonstração. Temos que $\frac{H_{i+1}}{H_i} \leq Z\left(\frac{G}{H_i}\right)$. Seja $h \in H_{i+1}$ e $g \in G$.

Daí, $[hH_i, gH_i] = H_i \Longrightarrow h^{-1}H_i\, g^{-1}H_i\, hH_i\, gH_i = [h,g]H_i = H_i \Longrightarrow [h,g] \in H_i$.

Logo, $[H_{i+1}, G] \leq H_i$.

□

Proposição 1.1.10. *Seja G um grupo nilpotente, e seja H um subgrupo de G. Então, $\forall\, i \geq 1$, $[H,G] \leq Z_i(G) \Longleftrightarrow H \leq Z_{i+1}$.*

Demonstração. Temos que $\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right)$, ou seja, $h \in Z_{i+1}(G) \Longleftrightarrow [hZ_i(G), gZ_i(G)] =$

$= Z_i(G) \Longleftrightarrow h^{-1}Z_i(G)\, g^{-1}Z_i(G)\, hZ_i(G)\, gZ_i(G) = [h,g]Z_i(G) = Z_i(G) \Longleftrightarrow [h,g] \in Z_i(G)$.

Logo, $[H,G] \leq Z_i(G) \Longleftrightarrow H \leq Z_{i+1}$.

□

Lema 1.1.11. *Seja $1 = H_0 \leq H_1 \leq \cdots \leq H_n = G$ uma série central de um grupo nilpotente G. Então $\gamma_i(G) \leq H_{n-i+1}$.*

Demonstração. Provemos por indução em i. Se $i = 1$, temos $G = \gamma_1(G) \leq H_n = G$. Suponhamos o resultado válido para i. Assim, pela proposição anterior, temos que $[H_{n-i+1}, G] \leq H_{n-i}$. Pela hipótese de indução, $\gamma_{i+1}(G) = [\gamma_i(G), G] \leq [H_{n-i+1}, G] \leq H_{n-i}$.

□

Lema 1.1.12. *G é nilpotente de classe c se, e somente se, $\gamma_{c+1}(G) = 1$ e $\gamma_c(G) \neq 1$.*

Demonstração. Seja G um grupo nilpotente de classe c, e seja $1 = H_0 \leq H_1 \leq \cdots \leq H_n = G$ uma série central de G. Pelo lema anterior, $\gamma_{c+1}(G) \leq H_0 = 1$. Logo, $\gamma_{c+1}(G) = 1$. Observemos que $\gamma_c(G) \neq 1$, pois a classe de nilpotência de G é c.

Por outro lado, seja $\gamma_{c+1}(G) = 1$ e $\gamma_c(G) \neq 1$. Daí, $G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_{c+1}(G) = 1$ é uma série central e, portanto, G é nilpotente.

□

Lema 1.1.13. *Seja $1 = H_0 \leq H_1 \leq \cdots \leq H_n = G$ uma série central de um grupo nilpotente G. Então $H_i \leq Z_i(G)$.*

Demonstração. Mostremos por indução. Para $i = 0$, temos $\{1\} = H_0 \leq Z_0(G) = \{1\}$. Seja agora $i > 0$. Pela hipótese de indução, $H_i \leq Z_i(G)$. Pela Proposição 1.1.9, temos $[H_{i+1}, G] \leq H_i \leq Z_i(G)$. Mas, pela proposição 1.1.10, temos $H_{i+1} \leq Z_{i+1}(G)$. □

Teorema 1.1.14. *Um grupo G é nilpotente de classe c se, e somente se, $Z_c(G) = G$ e $Z_{c-1}(G) \neq G$.*

Demonstração. Seja G nilpotente e seja $1 = H_0 \leq H_1 \leq \cdots \leq H_n = G$ uma série central de G. Então, pelo Lema 1.1.13, temos que $G = H_c \leq Z_c(G)$. Logo, $Z_c(G) = G$. Observemos que $Z_{c-1}(G) \neq G$, pois a classe de nilpotência de G é c.
Por outro lado, se $Z_c(G) = G$ e $Z_{c-1}(G) \neq G$, a série $1 = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_c(G) = G$ é uma série central, e portanto, G é nilpotente de classe c. □

Também podemos caracterizar os grupos nilpotentes finitos através do seguinte teorema:

Teorema 1.1.15. *Seja G um grupo finito. São equivalentes:*

(i) G é nilpotente;

(ii) $H \leq G$, então existem $K_0, ..., K_t$ tais que $K_0 = H \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_t = G$;

(iii) Se $H \lneqq G$, então $H \lneqq N_G(H)$;

(iv) Se M é um subgrupo maximal de G, então $M \trianglelefteq G$;

(v) G é produto direto dos seus subgrupos de Sylow.

As implicações que demonstram esse teorema podem ser encontradas em [5], pg. 130.

Capítulo 2

Resultados importantes acerca de p-grupos finitos

2.1 p-grupos finitos

Nesse capítulo, apresentaremos as definições de p-grupo finito e de p-grupo finito de classe maximal. Mostraremos que todo p-grupo finito é nilpotente, e então, apresentaremos alguns resultados acerca de nilpotência para os p-grupos finitos, e veremos alguns exemplos de p-grupos de classe maximal, além de definirmos centralizadores de dois passos.

Definição 2.1.1. *Seja G um grupo finito. G é um p-**grupo** se sua ordem é uma potência de um primo p, ou, equivalentemente, todos os seus elementos têm ordens potências de p.*

Lema 2.1.2. *Seja G um p-grupo finito, com $|G| = p^m$, $m \geq 1$. Então $|Z(G)| \neq 1$.*

Demonstração. Usando a equação das classes, temos que

$$|G| = |Z(G)| + \sum_{\substack{[x]\in G/C_G \\ |[x]|\neq 1}} |[x]| \quad = \quad |Z(G)| + \sum_{\substack{[x]\in G/C_G \\ x\notin Z(G)}} |G : C_G(x)|,$$

onde x corresponde a um representante de cada classe.

Daí, como p divide $|G|$, e p divide $|G : C_G(x)|$, para todo x, temos que p divide $|Z(G)|$. Logo, $|Z(G)| \neq 1$.

□

Teorema 2.1.3. *Todo p-grupo finito é nilpotente.*

Demonstração. Seja G um p-grupo finito. Suponhamos que, para algum índice i, tenhamos $Z_i(G) \neq G$. Sendo assim, tomemos $\frac{G}{Z_i(G)}$, que não é trivial. Pelo lema anterior, temos que $Z\left(\frac{G}{Z_i(G)}\right)$ também é não-trivial. Mas $Z\left(\frac{G}{Z_i(G)}\right) = \frac{Z_{i+1}(G)}{Z_i(G)}$ (não-trivial). Logo, a série central superior $1 = Z_0(G) < Z_1(G) = Z(G) < \cdots < Z_{k-1}(G) < Z_k(G)$ é estritamente crescente. Como G é finito, existe um natural k tal que $Z_k(G) = G$, e, como observado no Teorema 1.1.14, G é nilpotente. □

Teorema 2.1.4. *Seja G um p-grupo de ordem $p^m \geq p^2$. Então:*

(i) Se G tem classe de nilpotência c, então $|G : Z_{c-1}(G)| \geq p^2$;

(ii) A classe de nilpotência de G é, no máximo, $m - 1$;

(iii) $|G : G'| \geq p^2$.

Demonstração. ***(i)*** Suponhamos, por absurdo, que $|G : Z_{c-1}(G)| = p$. Sendo $c \geq 2$, temos $\frac{G/Z_{c-2}(G)}{Z(G/Z_{c-2}(G))} = \frac{G/Z_{c-2}(G)}{Z_{c-1}(G)/Z_{c-2}(G)} \cong \frac{G}{Z_{c-1}(G)}$, que é um grupo cíclico, pois tem ordem p.

Sabemos que um grupo G é abeliano se $\frac{G}{Z(G)}$ é cíclico. Portanto, temos que $\frac{G}{Z_{c-2}(G)}$ é abeliano. Notemos que, da série central superior, temos:

$\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right) \Longrightarrow \frac{Z_{c-1}(G)}{Z_{c-2}(G)} = Z\left(\frac{G}{Z_{c-2}(G)}\right) = \frac{G}{Z_{c-2}(G)}$. Logo, $Z_{c-1}(G) = G$,

o que é um absurdo, pois $|G : Z_{c-1}(G)| = p$. Portanto, $|G : Z_{c-1}(G)| \geq p^2$.

(ii) Da série central superior, temos $1 = Z_0(G) < Z_1(G) = Z(G) < \cdots < Z_{c-1}(G) < Z_c(G) = G$, com c passos. Pelo Teorema de Lagrange, temos que $|G| = \prod_{i=0}^{c-1} |Z_{i+1} : Z_i|$, e como $|Z_{i+1} : Z_i| \geq p$ se $i \neq c-1$, e $|Z_c : Z_{c-1}| \geq p^2$, temos que $|G| = p^m \geq p^{c+1}$. Logo, $c \leq m-1$.

(iii) Temos que $G' = \gamma_2(G) \leq Z_{c-1}(G)$, e, por (i), $|G : G'| \geq |G : Z_{c-1}(G)| \geq p^2$.

□

Corolário 2.1.5. *Seja G um p-grupo e seja N um subgrupo normal de G, de índice $p^i \geq p^2$. Então $\gamma_i(G) \leq N$.*

Demonstração. Nesse caso, o grupo G/N tem ordem $p^i \geq p^2$. Pelo Teorema anterior, G/N tem classe menor ou igual a $i - 1$, e, consequentemente, $\gamma_i(G/N)$ é trivial. Como

$\gamma_i(G/N) = \gamma_i(G)N/N$ (consequência do item (v) do Lema 1.1.4), temos que $\gamma_i(G) \leq N$.

□

Definição 2.1.6. *Um p-grupo finito de ordem $p^m \geq p^2$ é um* ***p-grupo de classe maximal*** *se sua classe de nilpotência é igual a $m-1$.*

São alguns exemplos de p-grupos de classe maximal os seguintes:

O grupo Diedral $D_{2^m} = \left\langle a, b \mid a^{2^{m-1}} = b^2 = 1, a^b = a^{-1} \right\rangle$;

O grupo Semi-diedral $SD_{2^m} = \left\langle a, b \mid a^{2^{m-1}} = b^2 = 1, a^b = a^{-1+2^{m-2}} \right\rangle$;

O grupo Quatérnio generalizado $Q_{2^m} = \left\langle a, b \mid a^{2^{m-1}} = 1, a^{2^{m-2}} = b^2, a^b = a^{-1} \right\rangle$;

O grupo $M_{p^3} = \left\langle a, b \mid a^{p^2} = b^p = 1, a^b = a^{p+1} \right\rangle$;

O grupo $E_{p^3} = \langle a, b, c \mid a^p = b^p = c^p = 1, ab = bac, ca = ac, bc = cb \rangle$.

Vamos verificar que o grupo $G = D_{2^m}$ é, de fato, de classe maximal.

De fato, pois temos $\gamma_2(G) = G' = \langle [a,b] \rangle^G$, pela Proposição 1.1.7.

Calculando, $[a,b] = a^{-1}a^b = a^{-2}$. Logo, $\gamma_2(G) = \langle a^2 \rangle$. Mostremos por indução que $\gamma_i(G) = \langle a^{2^{i-1}} \rangle$, para todo $i \geq 2$.
Seja $\gamma_{i-1}(G) = \langle a^{2^{i-2}} \rangle$. Temos $\gamma_i(G) = \langle [a^{2^{i-2}}, a], [a^{2^{i-2}}, b] \rangle^G = \langle [a^{2^{i-2}}, b] \rangle$. Calculando, $[a^{2^{i-2}}, b] = a^{-2^{i-2}}(a^{2^{i-2}})^b = a^{-2^{i-2}} \cdot a^{-2^{i-2}} = a^{-2^{i-1}}$.

Assim, $\gamma_i(G) = \langle a^{2^{i-1}} \rangle$. Desse modo, $\gamma_{m-1}(G) = \langle a^{2^{m-2}} \rangle \neq 1$,

e $\gamma_m(G) = \langle a^{2^{m-1}} \rangle = 1$. Logo, a classe de nilpotência de $G = D_{2^m}$ é $m-1$, ou seja, D_{2^m} é de classe maximal.

De maneira parecida, podemos mostrar que SD_{2^m} e Q_{2^m} são também de classe maximal.

No caso dos grupos $G = M_{p^3}$ e $G = E_{p^3}$, é fácil observar tal fato, pois ambos não são abelianos, logo $cl(G) \neq 1$, e, além disso, $cl(G) \leq 2$, pois $m = 3$. Portanto, $cl(G) = 2$.

Teorema 2.1.7. *Seja G um p-grupo de classe maximal de ordem p^m. Então:*

(i) $|G : G'| = p^2$ *e* $|\gamma_i(G) : \gamma_{i+1}(G)| = p$, *para* $2 \leq i \leq m-1$. *Consequentemente,* $|G : \gamma_i(G)| = p^i$, *para* $2 \leq i \leq m$;

(ii) Os únicos subgrupos normais de G *são os* $\gamma_i(G)$ *e os subgrupos maximais de* G, *isto é, se* N *é um subgrupo normal de* G, *de índice* $p^i \geq p^2$, *então* $N = \gamma_i(G)$;

(iii) $Z_i(G) = \gamma_{m-i}(G)$, *para* $0 \leq i \leq m-1$.

Demonstração. ***(i)*** Notemos que $p^m = |G| = |G : G'| \cdot \prod_{i=2}^{m-1} |\gamma_i(G) : \gamma_{i+1}(G)|$.

Mas, como $|\gamma_i(G) : \gamma_{i+1}(G)| \geq p$ e, pelo Teorema 2.1.11, $|G : G'| \geq p^2$, segue o resultado.

(ii) Seja N um subgrupo normal qualquer de G, e seja $|G : N| = p^i$, com $0 \leq i \leq m$. Daí, se $i = 0$, então $N = \gamma_1(G)$; Se $i = 1$, então N é maximal em G. Para $i \geq 2$, $\gamma_i(G) \leq N$, pelo Corolário 2.1.5. Como $|G : N| = p^i$, concluímos que $N = \gamma_i(G)$, pois, pela parte (i), $|G : \gamma_i(G)| = p^i$.

(iii) Novamente, pelo Teorema 2.1.11, $|G : Z_{m-2}(G)| \geq p^2$. Como

$|Z_{i+1}(G) : Z_i(G)| \geq p$, para $0 \leq i \leq m-3$, e

$$p^m = |G| = |G : Z_{m-2}(G)| \cdot \prod_{i=0}^{m-3} |Z_{i+1}(G) : Z_i(G)|,$$

todas as desigualdades acima tornam-se igualdades. Daí, $|G : Z_i(G)| = p^{m-i}$, para $0 \leq i \leq m-1$, e, pela parte (ii), $Z_i(G) = \gamma_{m-i}(G)$.

□

Uma das propriedades mais importantes da série central inferior é a seguinte:

Teorema 2.1.8. *: Para qualquer grupo* G, $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$, *para todo* $i, j \geq 1$.

Demonstração. Vamos provar por indução em i. Para $i = 1$, temos $[\gamma_1(G), \gamma_j(G)] = [G, \gamma_j(G)] \leq \gamma_{j+1}(G)$, da própria definição de $\gamma_i(G)$ na série central inferior. Suponhamos que o resultado é válido para $i-1$. Assim, $[\gamma_{i-1}(G), \gamma_j(G), G] \leq [\gamma_{i+j-1}(G), G] = \gamma_{i+j}(G)$. Também, $[\gamma_j(G), G, \gamma_{i-1}(G)] = [\gamma_{j+1}(G), \gamma_{i-1}(G)] \leq \gamma_{i+j}(G)$. Pelo Lema dos três subgrupos (Teorema 1.1.5), concluímos que $[\gamma_i(G), \gamma_j(G)] = [G, \gamma_{i-1}(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$.

□

Agora estamos interessados em estudar p-grupos de classe maximal. Como p-grupos de ordem menor ou igual a p^3 já estão classificados, vamos considerar apenas p-grupos de ordem p^m, com $m \geq 4$.

Definição 2.1.9. *Seja G um p-grupo de classe maximal, $|G| = p^m$, $m \geq 4$. Definimos o subgrupo G_1 como o centralizador de $\gamma_2(G)/\gamma_4(G)$, ou seja, $G_1 = \{x \in G \mid [x, g] \in \gamma_4(G), \forall g \in \gamma_2(G)\}$. G_1 é chamado de primeiro centralizador de dois passos. Mostraremos posteriormente que G_1 é um subgrupo característico e maximal de G.*

Lema 2.1.10. *Seja G um grupo. Então $\gamma_i(G)$ é característico em G, para todo $i \geq 1$.*

Demonstração. Façamos indução em i. Para $i = 1$, $\gamma_1(G) = G$ é, obviamente, característico em G. Agora, suponhamos o resultado válido para i, isto é, $\gamma_i(G)$ é característico em G. Temos que $\gamma_{i+1}(G) = [\gamma_i(G), G]$. Daí, $\gamma_{i+1}(G) = \left\langle [c_i, g] \mid c_i \in \gamma_i(G)\ , g \in G \right\rangle$. Seja φ um automorfismo de G. Pela hipótese de indução, temos que $\varphi(c_i) \in \gamma_i(G)$. Além disso, temos, obviamente, $\varphi(g) \in G$.
Dessa forma, temos $\varphi([c_i, g]) = \varphi(c_i^{-1}g^{-1}c_ig) = \varphi(c_i^{-1})\varphi(g^{-1})\varphi(c_i)\varphi(g) = [\varphi(c_i), \varphi(g)] \in [\gamma_i(G), G] = \gamma_{i+1}(G)$.
Seja agora $\varphi\left(\left\langle [c_i, g] \mid c_i \in \gamma_i(G)\ , g \in G \right\rangle\right) = \left\langle \varphi([c_i, g]) \mid c_i \in \gamma_i(G)\ , g \in G \right\rangle \subseteq \gamma_{i+1}(G)$. Logo, $\varphi(\gamma_{i+1}(G)) \subseteq \gamma_{i+1}(G)$, isto é, $\gamma_{i+1}(G)$ é característico em G. Portanto, $\gamma_i(G)$ é característico em G, $\forall\ i \geq 1$.

□

Lema 2.1.11. *Seja G um p-grupo de classe maximal tal que $|G| = p^m$, $m \geq 4$. Então G_1 é um subgrupo maximal e característico de G.*

Demonstração. Seja φ um automorfismo de G. Temos que $G_1 = C_G(\gamma_2(G)/\gamma_4(G))$, ou ainda, $G_1 = \{x \in G \mid [x, g] \in \gamma_4(G), \forall g \in \gamma_2(G)\}$. Pelo lema anterior, temos que G_2 e G_4 são característicos em G. Assim, seja $x \in G_1$. Daí, $[\varphi(x), G_2] = [\varphi(x), \varphi(G_2)] = \varphi([x, G_2]) \leq \varphi(G_4) = G_4$. Ou seja, $\varphi(x) \in G_1$, e, portanto, G_1 é característico em G.

Consideremos $G \neq G_1$, pois, caso contrário,

$G = C_G\left(\dfrac{\gamma_2(G)}{\gamma_4(G)}\right) \Longrightarrow [\gamma_1(G), \gamma_2(G)] = \gamma_3(G) \leq \gamma_4(G) \Longrightarrow \gamma_3(G) = \gamma_4(G)$ (já temos $\gamma_4(G) \leq \gamma_4(G)$).
Sendo assim, $\gamma_3(G) = \{1\} \Longrightarrow cl(G) \leq 2 \Longrightarrow |G| \leq p^3$, mas, por hipótese, $|G| \geq p^4$.

Vamos mostrar agora que G_1 é um subgrupo maximal de G. Seja f o seguinte homomorfismo:

$$f : G \longrightarrow \mathrm{Aut}\left(\frac{\gamma_2(G)}{\gamma_4(G)}\right)$$
$$gG_4 \longmapsto x^{-1}gx$$

Temos que $\ker f = \{x \in G \mid x^{-1}gx\ G_4 = gG_4, \forall g \in G_2\}$. Notemos que

$x^{-1}gx\,G_4 = g\,G_4 \iff g^{-1}x^{-1}gx\,\gamma_4(G) = \gamma_4(G) \iff x \in C_G\left(\frac{\gamma_2(G)}{\gamma_4(G)}\right) = G_1.$

Pelo primeiro teorema de homomorfismo, temos que $\frac{G}{G_1} = \frac{G}{\ker f} \cong \text{Im } f \leq \text{Aut}\left(\frac{\gamma_2(G)}{\gamma_4(G)}\right)$.

Temos que $\left|\frac{\gamma_2(G)}{\gamma_4(G)}\right| = p^2$. Daí, $\frac{\gamma_2(G)}{\gamma_4(G)} \cong \mathbb{Z}_{p^2}$ ou $\frac{\gamma_2(G)}{\gamma_4(G)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Se $\frac{\gamma_2(G)}{\gamma_4(G)} \cong \mathbb{Z}_{p^2}$, temos que

$|\text{Aut}(\mathbb{Z}_{p^2})| = p(p-1)$ (esse resultado pode ser encontrado em [4], pg. 27).

Como $G_1 \neq G$, e $\left|\frac{G}{G_1}\right|$ deve ser um múltiplo de p, segue que $\left|\frac{G}{G_1}\right| = p$, isto é, G_1 é um

subgrupo maximal de G.

Se $\frac{\gamma_2(G)}{\gamma_4(G)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, temos que $|\text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2-1)(p^2-p) = p(p-1)(p^2-1)$. ([4], pg. 30)

Pelo mesmo motivo anterior, temos que G_1 é um subgrupo maximal de G.

□

2.2 p-grupos regulares

Definição 2.2.1. *Seja G um p-grupo finito. Definimos $\Omega_i(G)$ como*

$$\Omega_i(G) = \langle x \in G \mid\ x^{p^i} = 1 \rangle, \text{ para todo } i \geq 0.$$

Definição 2.2.2. *Seja G um p-grupo finito. Definimos $\mho_i(G)$ como*

$$\mho_i(G) = \langle x^{p^i} \mid\ x \in G \rangle, \text{ para todo } i \geq 0.$$

Observação 2.2.3. *No caso de G ser abeliano, temos que $\Omega_i(G) = \{x \in G \mid\ x^{p^i} = 1\}$ e $\mho_i(G) = \{x^{p^i} \mid\ x \in G\}$, o que não acontece em geral.*

Teorema 2.2.4 (Fórmula de compilação de Hall)**.** *Sejam G um grupo e $x, y \in G$. Então existem elementos $c_i = c_i(x,y) \in \gamma_i(\langle x, y \rangle)$, tais que*

$$x^n y^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \cdots c_n^{\binom{n}{n}}$$

, para todo $n \in \mathbb{N}$.

Esse teorema está provado em [2], pg. 20.

Definição 2.2.5. *Seja G um p-grupo finito. Dizemos que G é um p-grupo regular se*

$$x^p y^p \equiv (xy)^p \ (mod\ \mathfrak{O}_1(\langle x, y\rangle')), \text{ para todo } x, y \in G.$$

Equivalentemente, se $c_p(x, y) \in \mathfrak{O}_1(\langle x, y\rangle')$, para todo $x, y \in G$.

Teorema 2.2.6. *Seja G um p-grupo regular e sejam $x, y \in G$. Então $x^p = y^p$ se, e somente se, $(x^{-1}y)^p = 1$.*

Demonstração. Como G é regular, temos que, para todo $x, y \in G$, $x^{-p}y^p = (x^{-1}y)^p z$, com $z \in \mathfrak{O}_1(\langle x, y\rangle')$. Dessa forma, é suficiente mostrar que, se $x^p = y^p$ ou $(x^{-1}y)^p = 1$, temos $\mathfrak{O}_1(\langle x, y\rangle') = 1$.

Supondo $x^p = y^p$, temos que y e x^p comutam e, portanto, $(x^p)^y = 1 = (x^y)^p$. Vamos mostrar por indução em $|H|$. Seja $H = \langle x, y\rangle$. Se H for cíclico, já está provado. Então suponhamos H não-cíclico, e existe um subgrupo maximal M de H, contendo x. Mas, como M é normal em H, então, se $x \in M$, $x^y \in M$. Logo, $\langle x, x^y\rangle \leq M$ e, como $|M| \leq |H|$, temos que $(x^{-1}x^y)^p = 1$ e $[x, y]^p = 1$, e H' é gerado por elementos de ordem p. Como $|H'| < |H|$, usando a hipótese indução, como o produto de elementos de ordem p tem ainda ordem p, temos que $\mathfrak{O}_1(\langle x, y\rangle') = 1$.

Supondo agora que $(x^{-1}y)^p = 1$, temos que $x(x^{-1}y)^p x^{-1} = 1$, o que implica que $(xx^{-1}yx^{-1})^p = 1$ e $(yx^{-1})^p = 1$. Pela implicação acima, $((yx^{-1})^{-1}x^{-1}y)^p = 1 = (xy^{-1}x^{-1}y)^p = [x^{-1}, y]^p$ e $H' = \langle [x^{-1}, y]^h \mid h \in H\rangle$. Novamente, como o produto de elementos de ordem p tem ainda ordem p, temos que $\mathfrak{O}_1(H') = 1$.

□

Teorema 2.2.7. *Seja G um p-grupo regular. Então:*

(i) Para todo $x, y \in G$ e para todo $i \geq 0$, temos que $x^{p^i} = y^{p^i}$ se, e somente se, $(x^{-1}y)^{p^i}$.

(ii) Para todo $i \geq 0$, $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.

(iii) Para todo $i \geq 0$, $\mathfrak{O}_i(G) = \{x^{p^i} \mid x \in G\}$.

(iv) Para todo $i \geq 0$, $|G : \Omega_i(G)| = |\mathfrak{O}_i(G)|$. (Consequentemente, também $|G : \mathfrak{O}_i(G)| = |\Omega_i(G)|$)

(v) Para todo $x, y \in G$, $[x^{p^i}, y^{p^j}] = 1 \iff [x, y]^{p^{i+j}} = 1$.

A prova do teorema acima encontra-se em [2], pg. 23.

Teorema 2.2.8. *Seja G um p-grupo finito.*

(i) Se a classe de G é menor que p, então G é regular. Em particular, todo p-grupo de ordem $\leq p^p$ é regular.

(ii) Se $\gamma_{p-1}(G)$ é cíclico, então G é regular. Portanto, se $p > 2$ e G' é cíclico, então G é regular.

(iii) Um 2-grupo regular é abeliano.

(iv) Se $|G : \mho_1(G)| \leq p^{p-1}$, então G é regular.

Podemos encontrar a prova desse resultado em [2], pg. 21.

Teorema 2.2.9. *Seja G um p-grupo de classe maximal de ordem $p^m \geq p^{p+2}$. Então:*

(i) G_1 é regular.

(ii) $\mho_1(G_i) = G_{i+p-1}$, $\forall\ i \geq 1$.

(iii) Se $1 \leq i \leq m-p$ e $x \in G_i - G_{i+1}$, então $x^p \in G_{i+p-1} - G_{i+p}$.

A demonstração desse teorema pode ser encontrada em [2], pg. 49.

2.3 Grau de comutatividade

Nos p-grupos de classe maximal é possível definir uma série
$G = G_0 > G_1 > G_2 > G_3 > .... > G_{m-1} = 1$, onde $G_i = \gamma_i(G)$ para $i \geq 2$, com $\gamma_i(G)$ sendo o i-ésimo termo da série central inferior. Também é possível mostrar que o subgrupo comutator $[G_i, G_j]$ está sempre contido em G_{i+j}, $\forall i, j \geq 1$. Logo, faz sentido estudar os valores de k, $0 \leq k \leq m-2$, tais que $[G_i, G_j] \leq G_{i+j+k}$ para todo i e j maiores ou iguais a 1.

Definição 2.3.1. *Seja G um p-grupo de classe maximal, $|G| = p^m$, $m \geq 4$. Definimos o **grau de comutatividade de** G, o qual indicamos com $l(G)$ (ou, de forma suscinta, por l), o natural k tal que $l(G) = max\{k \leq m-2 \mid [G_i, G_j] \leq G_{i+j+k}, \forall i, j \geq 1\}$.*

Informações sobre o grau de comutatividade se traduzem em informações sobre a estrutura do grupo. Por exemplo, temos que $l(G) = m-2$ se, e somente se, G_1 é abeliano. Também, temos que G_2 é abeliano quando $p = 3$, e tem classe de nilpotência, no máximo, 2, se $p = 5$. O estudo principal será sobre limitações do grau de comutatividade em função do primo p.

No estudo dos p-grupos de classe maximal, primeiro vamos considerar casos particulares, por exemplo, tomando p pequeno. Então primeiro estudamos 2-grupos de classe maximal. Felizmente conhecemos (a menos de isomorfismos) todos os 2-grupos de classe maximal. No seguinte teorema, temos uma identificação de tais grupos.

Teorema 2.3.2. *Seja G um 2-grupo de classe maximal. Então G é isomorfo a um desses grupos:*

$$D_{2^m} = \left\langle a, b \mid a^{2^{m-1}} = b^2 = 1, a^b = a^{-1} \right\rangle,$$
$$SD_{2^m} = \left\langle a, b \mid a^{2^{m-1}} = b^2 = 1, a^b = a^{-1+2^{m-2}} \right\rangle \text{ ou}$$
$$Q_{2^m} = \left\langle a, b \mid a^{2^{m-1}} = 1, a^{2^{m-2}} = b^2, a^b = a^{-1} \right\rangle.$$

A demonstração desse resultado pode ser encontrada em [2], pg. 55.

Através do estudo do grau de comutatividade obtemos informações sobre os 3-grupos e os 5-grupos, como podemos ver nos resultados abaixo:

Teorema 2.3.3. *Seja G um 3-grupo de classe maximal de ordem 3^m. Então $l(G) \geq m-4$. Consequentemente, G_1 tem classe de nilpotência ≤ 2, G_2 é abeliano e G tem comprimento derivado ≤ 2, ou seja, G é metabeliano.*

O Teorema a seguir nos dá uma limitação inferior para o grau de comutatividade de um 5-grupo de classe maximal de ordem 5^m.

Teorema 2.3.4. *Seja G um 5-grupo de classe maximal de ordem 5^m. Então $l(G) \geq \frac{m-6}{2}$. Consequentemente, G_1 tem classe de nilpotência ≤ 3, G_2 tem classe de nilpotência ≤ 2 e G tem comprimento derivado ≤ 3.*

As demonstrações desses resultados podem ser encontradas em [2], pg. 55–58.

Nosso objetivo agora é estudar os p-grupos de classe maximal, com $p \geq 7$. Para tal, introduziremos alguns conceitos e resultados importantes.

2.4 Elementos uniformes

Seja G um p-grupo de classe maximal de ordem p^m. Do mesmo modo que definimos o *primeiro centralizador de dois passos*, $G_1 = C_G(\gamma_2(G)/\gamma_4(G))$, vamos definir, de maneira geral, os *centralizadores de dois passos* $C_G(\gamma_i(G)/\gamma_{i+2}(G))$, $1 \leq i \leq m-2$. Assim como G_1, todos esses grupos são maximais e característicos em G. Como definido antes, $G_i = \gamma_i(G)$, para $i \geq 2$, com $\gamma_i(G)$ sendo o i-ésimo termo da série central inferior. Assim, temos que $[G_i : G_{i+1}] = p$. Dessa forma, G_i/G_{i+1} é cíclico e, portanto, $[G_i, G_{i+1}] = [G_i, G_i]$, como mostraremos no lema a seguir. Em particular, $[G_1, G_1] = [G_1, G_2] \leq G_4 \leq G_3$. Daí, temos que $C_G(G_1/G_3) \geq G_1$, e, sendo eles maximais, $C_G(G_1/G_3) = G_1$. Então, basta considerarmos os centralizadores de dois passos $C_G(G_i/G_{i+2})$ com $2 \leq i \leq m-2$.

Lema 2.4.1. *Se G é um grupo qualquer e N é um subgrupo normal de G tal que G/N é cíclico, então $G' = [G, N]$.*

Demonstração. Seja $G/N = \langle xN \rangle$. Desse modo, todo elemento de G pode ser escrito como $g = x^r n$, com $n \in N$ e $r \in \mathbb{Z}$.
Sejam $g_1, g_2 \in G$. Assim, $[g_1, g_2] = [x^t n, x^s m] = [x^t, x^s m]^n [n, x^s m] =$
$= [x^t, m]^n [x^t, x^s]^{mn} [n, x^s m] \in [G, N]$. Daí, $[G, G] \leq [G, N] \leq [G, G]$ e, portanto, $G' = [G, N]$.
□

Definição 2.4.2. *Seja G um p-grupo de classe maximal de ordem p^m, $m \geq 4$. Um elemento $s \in G$ é chamado elemento uniforme se $s \notin \bigcup_{i=2}^{m-2} C_G(G_i/G_{i+2})$.*

A existência de elementos uniformes em qualquer p-grupo de classe maximal, que é equivalente a afirmar que $G \neq \bigcup_{i=2}^{m-2} C_G(G_i/G_{i+2})$, é garantida pelo item (iii) do seguinte teorema:

Teorema 2.4.3 (Teorema de Blackburn)**.** *Seja G um p-grupo de classe maximal de ordem p^m. Valem:*

(i) Se $l(G) \geq 0$, então $p \geq 5$, m é par e $6 \leq m \leq p+1$.

(ii) $l(G/Z(G)) \geq 1$.

(iii) G possui elementos uniformes.

A demonstração desse teorema pode ser encontrada em [1].

Lema 2.4.4. *Seja G um p-grupo de classe maximal de ordem p^m, e seja s um elemento uniforme em G. Se $1 \leq i \leq m-2$ e $x \in G_i - G_{i+1}$, então $[s,x] \in G_{i+1} - G_{i+2}$.*

Demonstração. Como $x \in G_i$, temos que $[s,x] \in G_{i+1}$. Assim, basta provar que $[s,x] \notin G_{i+2}$. Por absurdo, suponhamos que $[s,x] \in G_{i+2}$. Seja $\overline{G} = G/G_{i+2}$, o que significa que $\overline{s}$ e $\overline{x}$ comutam em $\overline{G}$. Temos também que $[s, G_{i+1}] \leq G_{i+2}$, isto é, $\overline{s}$ centraliza $\overline{G}_{i+1}$. Como $G_i = \langle x, G_{i+1} \rangle$, pois $|G_i : G_{i+1}| = p$, segue que $\overline{s}$ centraliza $\overline{G}_i$. Então $[s, G_i] \leq G_{i+2}$, e $s \in C_G(G_i/G_{i+2})$, o que contradiz o fato de s ser um elemento uniforme. □

2.5 Cadeias e a função α associada

Seja G um p-grupo de classe maximal, s um elemento uniforme e $s_1 \in G_1 - G_2$. Definindo recursivamente $s_i = [s_{i-1}, s]$, $\forall i \geq 2$, dizemos que a sequência de elementos $\{s, s_1, s_2, ...\}$ é uma cadeia em G. É importante ressaltar que a existência de um elemento uniforme é equivalente à existência de uma cadeia. Temos que, se $\{s, s_1, s_2, ...\}$ é uma cadeia em G, e $\overline{G}$ é um quociente de G de ordem maior ou igual a p^4, então $\{\overline{s}, \overline{s_1}, \overline{s_2}, ...\}$ é uma cadeia em $\overline{G}$. Devemos ter $|\overline{G}| \geq p^4$, pois, toda a teoria desenvolvida nesse estudo é para p-grupos finitos G de ordem p^m, com $m \geq 4$. Assim, denotando o elemento uniforme s por s_0, temos que $s_i \in G_i - G_{i+1}$, para $0 \leq i \leq m-1$ e $s_i = 1$ para $i \geq m$. Ainda, podemos observar que $s_i G_{i+1} \in G_i/G_{i+1} = \langle s_i G_{i+1} \rangle$. Daí, como $[s_i, s_j] \in G_{i+j+l}$, temos que $[s_i, s_j]\, G_{i+j+l+1} \in \dfrac{G_{i+j+l}}{G_{i+j+l+1}} = \left\langle s_{i+j+l} G_{i+j+l+1} \right\rangle$. Então existe $\alpha(i,j) \in \mathbb{Z}$ tal que $[s_i, s_j]$

$G_{i+j+l+1} = s_{i+j+l}^{\alpha(i,j)} G_{i+j+l+1}$, para qualquer par de índices $i, j \geq 1$ tais que $i + j + l \leq m - 1$, onde $l = l(G)$ é o grau de comutatividade, e

$$\begin{aligned} \alpha : \{(i,j) \in \mathbb{N}^{*^2} \mid i + j \leq m - l - 1\} &\longrightarrow \mathbb{Z}_p \\ (i,j) &\longmapsto \alpha(i,j). \end{aligned}$$

está bem definida.

Ou, em termos de congruência,

$$[s_i, s_j] \equiv s_{i+j+l}^{\alpha(i,j)} \pmod{G_{i+j+l+1}}$$

para algum inteiro $\alpha(i,j)$, que é unicamente determinado módulo p, podendo ser considerado um elemento de $\mathbb{Z}_p$. A fim de que o domínio da função α seja não-vazio, impomos a condição $l(G) < m - 2$. Também, da própria definição do grau de comutatividade, α não pode ser a função nula, pois, nesse caso, teríamos

$$[s_i, s_j]\, G_{i+j+l+1} = G_{i+j+l+1}, \forall\ i, j \text{ no domínio de } \alpha.$$

Ou seja, $[G_i, G_j] \leq G_{i+j+l+1}$, $\forall\ i, j$, e l não seria o máximo k da definição de grau de comutatividade.

A função α satsisfaz algumas propriedades para valores de i, j onde a função está definida. São elas:

(P_1) $\alpha \not\equiv 0$

(P_2) $\alpha(i,i) = 0$, para $2i \leq m - l - 1$.

(P_3) $\alpha(i,j) = -\alpha(j,i)$, para $i + j \leq m - l - 1$

(P_4) $\alpha(i,j) = \alpha(i+1,j) + \alpha(i,j+1)$, para $i + j \leq m - l - 2$

(P_5) $\alpha(i,i+2) = \alpha(i,i+1)$, para $2i \leq m - l - 3$

(P_6) Seja $\Gamma_\alpha(i,j,k) = \alpha(i,j)\alpha(i+j+l,k) + \alpha(j,k)\alpha(j+k+l,i) + \alpha(k,i)\alpha(k+i+l,j)$. Então $\Gamma_\alpha(i,j,k) = 0$, para $i + j + k \leq m - 2l - 1$.

(P_7) $\alpha(i,j) = \alpha(i+p-1,j) = \alpha(i,j+p-1)$, para $i + j \leq m - l - p$

Lema 2.5.1. *Seja uma cadeia $\{s_i\} \in G$. Então $s_i^p \equiv s_{i+p-1}^{-1}$ (mod G_{i+p}), para todo $i \geq 1$.*

O lema acima é um lema técnico, e sua prova pode ser vista em [2], pg 51.

2.6 Demonstração das propriedades de α

Antes de provarmos as propriedades da função α, vamos ver um resultado que será bastante útil no que segue.

Lema 2.6.1. *Seja G um grupo. Se $[a,b,b]=1$, então $[a,b^n]=[a,b]^n$, $\forall\ n\in\mathbb{Z}$.*

Demonstração. Vamos mostrar o resultado usando indução sobre n. Para $n=1$, é imediato que vale o resultado. Suponhamos o resultado válido para $k>1$, isto é, $[a,b^k]=[a,b]^k$. Daí, seja $[a,b^{k+1}]=[a,b.b^k]=[a,b^k].[a,b]^{b^k}=[a,b^k].[a,b]=[a,b]^k.[a,b]=[a,b]^{k+1}$.

Seja agora $n=-1$. Assim, $[a,b]^{-1}=[b,a]=[b,a].bb^{-1}=b[b,a]b^{-1}=bb^{-1}a^{-1}bab^{-1}=$

$=[a,b^{-1}]$. Logo, se $n<-1$, $[a,b^n]=[a,b^{(-1).(-n)}]=[a,b^{-1}]^{-n}=[a,b]^n$.

□

Vamos mostrar agora a validade das propriedades de α:

Demonstração. Seja $[s_i,s_j]\equiv s_{i+j+l}^{\alpha(i,j)}\pmod{G_{i+j+l+1}}$.

(P_1) Segue pela definição de grau de comutatividade.

(P_2) Temos que $[s_i,s_i]=1$, isto é, $[s_i,s_i]\,G_{2i+l+1}=s_{2i+l}^{0}\,G_{2i+l+1}$. Logo, $\alpha(i,i)=0$

(P_3) Observemos que $[s_i,s_j]=[s_j,s_i]^{-1}$.

Temos $[s_i,s_j]\,G_{i+j+l+1}=s_{i+j+l}^{\alpha(i,j)}\,G_{i+j+l+1}$ e $[s_j,s_i]\,G_{i+j+l+1}=s_{i+j+l}^{\alpha(j,i)}\,G_{i+j+l+1}$.

Logo, $\left(s_{i+j+l}^{\alpha(i,j)}\right)\,G_{i+j+l+1}=\left(s_{i+j+l}^{\alpha(j,i)}\right)^{-1}\,G_{i+j+l+1}$, isto é, $\alpha(i,j)=-\alpha(j,i)$.

(P_4) Pela Identidade de Hall-Witt, $[s_0,s_i^{-1},s_j]^{s_i}\,.\,[s_i,s_j^{-1},s_0]^{s_j}\,.\,[s_j,s_0^{-1},s_i]^{s_0}=1$,

ou seja, $[s_0,s_i^{-1},s_j]^{s_i}\,.\,[s_i,s_j^{-1},s_0]^{s_j}\,.\,[s_j,s_0^{-1},s_i]^{s_0}\,G_{i+j+l+2}=G_{i+j+l+2}$.

Temos que $[s_0,s_i^{-1},s_j]\in G_{i+j+l+1}$.

Logo, $[s_0,s_i^{-1},s_j]^{s_i}\,.\,[s_i,s_j^{-1},s_0]^{s_j}\,.\,[s_j,s_0^{-1},s_i]^{s_0}\,G_{i+j+l+2}\in\dfrac{G_{i+j+l+1}}{G_{i+j+l+2}}$.

$[s_0, s_i^{-1}, s_j]\, G_{i+j+l+2}$, $[s_i, s_j^{-1}, s_0]\, G_{i+j+l+2}$, $[s_j, s_0^{-1}, s_i]\, G_{i+j+l+2} \in Z\left(\frac{G}{G_{i+j+l+2}}\right)$.

Portanto, $[s_0, s_i^{-1}, s_j]\, G_{i+j+l+2}$ comuta com $s_i\, G_{i+j+l+2}$ e, então,

$[s_0, s_i^{-1}, s_j]^{s_i}\, G_{i+j+l+2} = [s_0, s_i^{-1}, s_j]\, G_{i+j+l+2}$.

O mesmo vale para $[s_i, s_j^{-1}, s_0]^{s_j}\, G_{i+j+l+2}$ e $[s_j, s_0^{-1}, s_i]^{s_0}\, G_{i+j+l+2}$.

Como $[s_0, s_i^{-1}] \in G_{i+1}$, temos que $[[s_0, s_i], s_i]G_{i+2} = G_{i+2}$, pois $\frac{G_{i+1}}{G_{i+2}} \leq Z\left(\frac{G}{G_{i+2}}\right)$.

Pelo Lema 2.6.1, $[s_0, s_i^{-1}] = [s_0, s_i]^{-1} \pmod{G_{i+2}}$, ou ainda, $[s_0, s_i^{-1}] = [s_0, s_i]^{-1}.g$,

com $g \in G_{i+2}$. Daí, $[s_0, s_i^{-1}, s_j] = [[s_0, s_i]^{-1}.g, s_j] = [[s_0, s_i]^{-1}, s_j]^g.[g, s_j]$ (Lema 1.1.4).

Desse modo, temos que $[[s_0, s_i]^{-1}, s_j]^g.[g, s_j] = [[s_0, s_i]^{-1}, s_j] \bmod(G_{i+j+l+2})$,

pois $[[s_0, s_i]^{-1}, s_j] \in Z\left(\frac{G}{G_{i+j+l+2}}\right)$ e $[g, s_j] \in G_{i+j+l+2}$.

Pelo mesmo motivo, temos também que $[[[s_0, s_i], s_j], [s_0, s_i]]\, G_{i+j+l+2} = G_{i+j+l+2}$.

Novamente pelo Lema 2.6.1, $[s_0, s_i^{-1}, s_j]\, G_{i+j+l+2} = [[s_0, s_i^{-1}], s_j]\, G_{i+j+l+2} =$

$= [[s_0, s_i]^{-1}, s_j]\, G_{i+j+l+2} = [s_0, s_i, s_j]^{-1}\, G_{i+j+l+2}$. Assim,

$[s_0, s_i^{-1}, s_j]^{s_i}\, G_{i+j+l+2} = [s_0, s_i, s_j]^{-1}\, G_{i+j+l+2}$. Os outros dois são análogos.

Portanto, temos $[s_0, s_i, s_j]^{-1}\, .\, [s_i, s_j, s_0]^{-1}\, .\, [s_j, s_0, s_i]^{-1}\, G_{i+j+l+2} = G_{i+j+l+2}$,

ou ainda, $[s_0, s_i, s_j]^{-1}\, G_{i+j+l+2}\, .\, [s_i, s_j, s_0]^{-1}\, G_{i+j+l+2}\, .\, [s_j, s_0, s_i]^{-1}\, G_{i+j+l+2} = G_{i+j+l+2}$.

Como $[s_0, s_i] = [s_i, s_0]^{-1} = s_{i+1}^{-1}$, e, além disso, temos $[s_i, s_j] \equiv s_{i+j+l}^{\alpha(i,j)} \pmod{G_{i+j+l+1}}$,

(ou $[s_i, s_j]\, G_{i+j+l+1} = s_{i+j+l}^{\alpha(i,j)}\, G_{i+j+l+1}$), temos:

$[s_0, s_i, s_j]^{-1}\, G_{i+j+l+2} = [s_{i+1}^{-1}, s_j]^{-1}\, G_{i+j+l+2} = s_{i+j+l+1}^{\alpha(i+1,j)}\, G_{i+j+l+2}$;

$[s_i, s_j, s_0]^{-1}\, G_{i+j+l+2} = [s_{i+j+l}^{\alpha(i,j)}, s_0]^{-1}\, G_{i+j+l+2} = s_{i+j+l+1}^{-\alpha(i,j)}\, G_{i+j+l+2}$;

$[s_j, s_0, s_i]^{-1}\, G_{i+j+l+2} = [s_{j+1}, s_i]^{-1}\, G_{i+j+l+2} = s_{i+j+l+1}^{-\alpha(j+1,i)}\, G_{i+j+l+2}$.

Portanto, $[s_0, s_i, s_j]^{-1}\, G_{i+j+l+2}$. $[s_i, s_j, s_0]^{-1}\, G_{i+j+l+2}$. $[s_j, s_0, s_i]^{-1}\, G_{i+j+l+2} = G_{i+j+l+2}$

$\Longrightarrow s_{i+j+l+1}^{\alpha(i+1,j)}\, G_{i+j+l+2}$. $s_{i+j+l+1}^{-\alpha(i,j)}\, G_{i+j+l+2}$. $s_{i+j+l+1}^{-\alpha(j+1,i)}\, G_{i+j+l+2} = G_{i+j+l+2}$

$\Longrightarrow s_{i+j+l+1}^{\alpha(i+1,j)}$. $s_{i+j+l+1}^{-\alpha(i,j)}$. $s_{i+j+l+1}^{-\alpha(j+1,i)}\, G_{i+j+l+2} = G_{i+j+l+2}$

$\Longrightarrow \alpha(i+1, j) - \alpha(i, j) - \alpha(j+1, i) = 0$

$\Longrightarrow \alpha(i, j) = \alpha(i, j+1) + \alpha(i+1, j)$.

(P_5) Segue diretamente de P_4 e de P_2

(P_6) Novamente, temos $[s_i, s_j^{-1}, s_k]^{s_j}$. $[s_j, s_k^{-1}, s_i]^{s_k}$. $[s_k, s_i^{-1}, s_j]^{s_i} = 1$.

Usando o mesmo raciocínio da prova de P_4, temos

$[s_i, s_j, s_k]^{-1}$. $[s_j, s_k, s_i]^{-1}$. $[s_k, s_i, s_j]^{-1}\, G_{i+j+l+2} = G_{i+j+l+2}$.

Por definição, temos $[s_i, s_j] \equiv s_{i+j+l}^{\alpha(i,j)} \pmod{G_{i+j+l+1}}$.

Daí, $[s_i, s_j, s_k]^{-1} = [s_{i+j+l}^{\alpha(i,j)}.t, s_k]^{-1}$ (com $t \in G_{i+j+l+1}$) $= [s_{i+j+l}^{\alpha(i,j)}, s_k]^{-1} =$

$= [s_{i+j+l}, s_k]^{-\alpha(i,j)} = \left(s_{i+j+k+2l}^{\alpha(i+j+l,k)}\right)^{-\alpha(i,j)} = s_{i+j+k+2l}^{-\alpha(i,j)\alpha(i+j+l,k)}$.

Para os outros dois fatores, o raciocínio é análogo.

Sendo assim, temos que

$s_{i+j+k+2l}^{-\alpha(i,j)\alpha(i+j+l,k)}$. $s_{i+j+k+2l}^{-\alpha(j,k)\alpha(j+k+l,i)}$. $s_{i+j+k+2l}^{-\alpha(k,i)\alpha(k+i+l,j)}\, G_{i+j+k+2l+1} = G_{i+j+k+2l+1}$.

Portanto, $-\alpha(i, j)\alpha(i + j + l, k) - \alpha(j, k)\alpha(j + k + l, i) - \alpha(k, i)\alpha(k + i + l, j) = 0$

$\Longrightarrow \Gamma_\alpha(i, j, k) = \alpha(i, j)\alpha(i + j + l, k) + \alpha(j, k)\alpha(j + k + l, i) + \alpha(k, i)\alpha(k + i + l, j) = 0.$

□

Observação 2.6.2. *A demonstração da propriedade (P_7) será apresentada em forma de um teorema, pois usaremos algumas ferramentas de grupos regulares.*

Teorema 2.6.3. *(Propriedade P_7). Seja G um p-grupo de classe maximal de ordem maior ou igual a p^{p+2}. Consideremos a cadeia $\{s_i\} \in G$, e seja α sua função associada.*
Então $\alpha(i,j) = \alpha(i+p-1, j) = \alpha(i, j+p-1)$, para $i + j \leq m - l - p$.

Demonstração. Consideremos o comutador $[s_i^p, s_j] = s_i^{-p} s_j^{-1} s_i^p s_j = s_i^{-p} (s_i^{s_j})^p$. Notemos que

s_i e $s_j \in G_1$. Como G_1 é regular, temos que $[s_i^p, s_j] \equiv [s_i, s_j]^p \pmod{\mho_1(H')}$, onde

$H = \langle s_i^{-1}, s_i^{s_j} \rangle$. Observemos que $H = \langle s_i, [s_i, s_j] \rangle$. Como esses dois geradores

comutam módulo $G_{i+j+l+1}$, como vimos na demonstração da propriedade anterior,

segue que $H' \leq G_{i+j+l+1}$ e, consequentemente, $[s_i^p, s_j] \equiv [s_i, s_j]^p \pmod{G_{i+j+l+1}}$.

Pela definição de $\alpha(i,j)$, temos $[s_i, s_j] \equiv s_{i+j+l}^{\alpha(i,j)} \pmod{G_{i+j+l+1}}$, e, pela regularidade de G_1,

$[s_i, s_j]^p \equiv s_{i+j+l}^{p\alpha(i,j)} \pmod{G_{i+j+l+1}}$. De fato, pois

$$\begin{aligned}
[s_i, s_j]\, G_{i+j+l+1} &= s_{i+j+l}^{\alpha(i,j)}\, G_{i+j+l+1} \\
&\Longrightarrow [s_i, s_j]^{-1} \,.\, s_{i+j+l}^{\alpha(i,j)} \in G_{i+j+l+1} \\
\text{(por (ii) do Lema 2.2.9)} &\Longrightarrow \left([s_i, s_j]^{-1} \,.\, s_{i+j+l}^{\alpha(i,j)}\right)^p \in G_{i+j+l+p} \\
\text{(pelo Teorema 2.2.6)} &\Longrightarrow [s_i, s_j]^p\, G_{i+j+l+p} = s_{i+j+l}^{p\alpha(i,j)}\, G_{i+j+l+p}.
\end{aligned}$$

Pelo Lema 2.5.1, $s_{i+j+l}^p \equiv s_{i+j+l+p-1}^{-1} \pmod{G_{i+j+l+p}} \Longrightarrow$

$\Longrightarrow s_{i+j+l}^{p\alpha(i,j)} \equiv s_{i+j+l+p-1}^{-\alpha(i,j)} \pmod{G_{i+j+l+p}}$. Logo, $[s_i^p, s_j] \equiv s_{i+j+l+p-1}^{-\alpha(i,j)} \pmod{G_{i+j+l+p}}$.

Por outro lado, $s_i^p \equiv s_{i+p-1}^{-1} \pmod{G_{i+p}}$.

Notemos que $s_i^p \equiv s_{i+p-1}^{-1} \pmod{G_{i+p}} \Longrightarrow s_i^p\, G_{i+p} = s_{i+p-1}^{-1}\, G_{i+p}$, ou seja,

$\exists\, k \in G_{i+p}$ tal que $s_i^p = k \,.\, s_{i+p-1}^{-1}$.

Daí, $[s_i^p, s_j] = [k \,.\, s_{i+p-1}^{-1}, s_j] = [k, s_j]^{s_{i+p-1}} \,.\, [s_{i+p-1}^{-1}, s_j] = [s_{i+p-1}^{-1}, s_j]$.

Portanto, $[s_i^p, s_j] \equiv [s_{i+p-1}^{-1}, s_j] \equiv [s_{i+p-1}, s_j]^{-1} \equiv s_{i+j+l+p-1}^{-\alpha(i+p-1,j)} \pmod{G_{i+j+l+p}}$.

Comparando as duas expressões obtidas para $[s_i^p, s_j]$, segue que $\alpha(i+p-1, j) = \alpha(i, j)$.

Ainda, pela propriedade P_3, $\alpha(i, j) = -\alpha(j, i) = -\alpha(j + p - 1, i) = \alpha(i, j + p - 1)$.

□

O teorema a seguir nos permite obter qualquer valor de $\alpha(i, j)$ a partir de valores particulares da forma $\alpha(r, r + 1)$. A fim de tornar mais clara a escrita da demonstração desse teorema, introduzimos a seguinte definição:

Definição 2.6.4. *Chamamos de coeficientes binomiais generalizados uma extensão dos coeficientes binomiais que é da forma*

$$\binom{n}{k} = \begin{cases} \dfrac{n(n-1)\cdots(n-k+1)}{k!}, & se \quad k \geq 1; \\ 1, & se \quad k = 0; \\ 0, & se \quad k < 0. \end{cases} \qquad \forall n, k \in \mathbb{Z}.$$

Para esses coeficientes generalizados, ainda temos válidas as propriedades

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \qquad \text{e} \qquad \binom{n}{k} = \binom{n}{n-k}, \text{ no caso de } n \geq 0, \text{ e}$$

$$\binom{n}{k} = 0, \text{ para } 0 \leq n < k.$$

Teorema 2.6.5. *Seja G um p-grupo de classe maximal de ordem p^m e $l(G) < m - 2$. Seja α a função associada a uma cadeia de G. Seja $x_r = \alpha(r, r + 1)$ então*

$$\alpha(i, j) = \sum_{r=i}^{\lfloor \frac{i+j-1}{2} \rfloor} (-1)^{r-i} \binom{j-r-1}{r-i} x_r, \text{ para } i < j.$$

Demonstração. Usando os coeficientes binomiais generalizados, podemos escrever a expressão acima como

$$\alpha(i, j) = \sum_{r=i}^{j-1} (-1)^{r-i} \binom{j-r-1}{r-i} x_r.$$

Vamos fazer a demonstração usando indução em $j - i$. No caso de $j - i = 1$ ou $j - i = 2$, já temos válido o resultado, pois temos

$$\alpha(i, i+1) = \sum_{r=i}^{i} (-1)^{r-i}\binom{i+1-r-1}{r-i}x_r = \binom{0}{0}x_i = \alpha(i, i+1)$$

e, pela propriedade P_5 de α, $\alpha(i, i+1) = \alpha(i, i+2)$.
Suponhamos agora o resultado válido até $j - i - 1$. Pela propriedade P_4 de α,

$\alpha(i, j-1) = \alpha(i+1, j-1) + \alpha(i, j)$, ou ainda,

$$\begin{aligned}
\alpha(i,j) &= \alpha(i,j-1) - \alpha(i+1,j-1) \\
&= \sum_{r=i}^{j-2} (-1)^{r-i}\binom{j-r-2}{r-i}x_r - \sum_{r=i+1}^{j-2} (-1)^{r-i-1}\binom{j-r-2}{r-i-1}x_r \\
&= \sum_{r=i}^{j-2} (-1)^{r-i}\binom{j-r-2}{r-i}x_r + \sum_{r=i+1}^{j-2} (-1)^{r-i}\binom{j-r-2}{r-i-1}x_r \\
\text{(o termo com } r &= i+1\text{, no segundo somatório, vale 0)} \\
&= \sum_{r=i}^{j-2} (-1)^{r-i}\binom{j-r-2}{r-i}x_r + \sum_{r=i}^{j-2} (-1)^{r-i}\binom{j-r-2}{r-i-1}x_r \\
\text{(soma de coef. binomiais)} &= \sum_{r=i}^{j-2} (-1)^{r-i}\binom{j-r-1}{r-i}x_r \\
&= \sum_{r=i}^{j-1} (-1)^{r-i}\binom{j-r-1}{r-i}x_r.
\end{aligned}$$

Temos a última igualdade, pois

$(-1)^{j-1-i}\binom{j-(j-1)-1}{j-1-i}x_{j-1} = (-1)^{j-1-i}\binom{0}{j-1-i}x_{j-1} = 0$, uma vez que

$j - 1 - i > 0$.

□

Capítulo 3

Uma limitação inferior para o grau de comutatividade

3.1 Resultados de Leedham-Green e McKay

Lema 3.1.1 (Leedham-Green e McKay)**.** *Seja $p \geq 7$. Se tivermos $l(G) \leq \dfrac{m-3p+5}{2}$, então podemos estender a função α a uma função γ que cumpre as mesmas propriedades P_1 a P_7, e tem domínio $\mathbb{Z}^2$.*

Demonstração. Seja α a função associada a uma cadeia em G. Temos que

$$\begin{array}{rcl} \alpha : \{(i,j) \in \mathbb{N}^{*^2} \mid i+j \leq m-l-1\} & \longrightarrow & \mathbb{Z}_p \\ (i,j) & \longmapsto & \alpha(i,j). \end{array}$$

Vamos estender α a uma função $\gamma : \mathbb{Z} \times \mathbb{Z} \longmapsto \mathbb{Z}_p$, definida por $\gamma(i,j) \longmapsto \alpha(i_0, j_0)$, com $i_0 \equiv i (\text{mod } p-1)$ e $j_0 \equiv j (\text{mod } p-1)$, $1 \leq i_0, j_0 \leq p-1$.

Observemos que isso faz sentido, pois devemos ter $m-l-1 \geq i_0 + j_0$. Notemos que $i_0, j_0 \leq p-1$, então $i_0 + j_0 \leq 2p-2$. Como $l(G) \geq 0$, temos que $m \geq 3p-5$. Ainda, temos $p \geq 7$. Logo, $m \geq 3p-5 = 2p+p-5 \geq 14+p-5 = p+9$. Daí,

$$m-l-1 \geq m - \frac{m-3p+5}{2} - 1 = \frac{m+3p-7}{2} \geq \frac{p+9+3p-7}{2} \geq \frac{4p+2}{2} = 2p+1 > 2p-2.$$

Como α tem período $p-1$, para todo par (i,j) no domínio de α, $\gamma(i,j) = \alpha(i,j)$, o que indica que γ é uma extensão de α. É fácil verificar as propriedades P_1 a P_5, e P_7 para γ. A verificação da propriedade P_6 é um pouco mais delicada. Verificaremos a seguir.

Denotando $\Gamma_\gamma(i,j,k) := \gamma(i,j)\gamma(i+j+l,k) + \gamma(j,k)\gamma(j+k+l,i) + \gamma(k,i)\gamma(k+i+l,j)$, temos que $\Gamma_\gamma(i,j,k) = \Gamma_\gamma(i_0,j_0,k_0)$, pois vale a propriedade P_7. Se tivermos dois dos

valores i_0, j_0, k_0 iguais, obviamente $\Gamma_\gamma(i_0, j_0, k_0) = 0$. Dessa forma, podemos assumir que que i_0, j_0, k_0 são todos diferentes. Notemos que $2l \leq m - 3p - 5 \Rightarrow m - 2l \geq 3p - 5$. Logo, $m - 2l - 1 \geq 3p - 5 - 1 = 3p - 6$. Daí, temos que $i_0 + j_0 + k_0 \leq (p-1) + (p-2) + (p-3) = 3p - 6 \leq m - 2l - 1$, pois cada variável é menor ou igual a $p - 1$, e, além disso, devem ser todas diferentes. Dessa forma, temos que todos os valores aos quais aplicamos γ em $\Gamma_\gamma(i_0, j_0, k_0)$ estão no domínio de α. Assim, podemos estender α através de γ e $\Gamma_\gamma(i_0, j_0, k_0) = 0$ será uma consequência natural de P_6 para α.

□

Teorema 3.1.2 (Leedham-Green e McKay)**.** *Seja G um p-grupo de classe maximal de ordem p^m, $p \geq 7$. Então $l(G) \geq \dfrac{m - 3p + 6}{2}$.*

Demonstração. Por contradição, vamos supor que $l(G) \leq \dfrac{m - 3p + 5}{2}$. Vamos aplicar a propriedade P_6 a $(i, i+1, 1-l)$, com respeito à função γ, para um $i \in \mathbb{Z}$ arbitrário.

Assim,

$$\begin{aligned}
\Gamma_\gamma(i, i+1, 1-l) &= \gamma(i, i+1)\gamma(i+i+1+l, 1-l) + \gamma(i+1, 1-l)\gamma(i+1+1-l+l, i) + \\
&+ \gamma(1-l, i)\gamma(1-l+i+l, i+1) = 0 \\
&= \gamma(i, i+1)\gamma(2i+1+l, 1-l) + \gamma(i+1, 1-l)\gamma(i+2, i) = 0 \\
&= \gamma(i, i+1)\gamma(2i+1+l, 1-l) - \gamma(i+1, 1-l)\gamma(i, i+2) = 0 \\
&= \gamma(i, i+1)\gamma(2i+1+l, 1-l) - \gamma(i+1, 1-l)\gamma(i, i+1) = 0 \\
&= \gamma(i, i+1)\Big[\gamma(2i+1+l, 1-l) - \gamma(i+1, 1-l)\Big] = 0 \\
&= \gamma(i, i+1)\Big[-\gamma(1-l, 2i+1+l) + \gamma(1-l, i+1)\Big] = 0 \\
&= \gamma(i, i+1)\Big[\gamma(1-l, 2i+1+l) - \gamma(1-l, i+1)\Big] = 0
\end{aligned}$$

Como γ cumpre as mesmas propriedades que α, vale o Teorema 2.6.5. Daí, $\gamma(i, j)$ pode ser expresso por $x_r = \gamma(r, r+1)$. Assim, vamos calcular $\gamma(1-l, 2i+1+l)$ e $\gamma(1-l, i+1)$.

$$\begin{aligned}
\text{Como } \gamma(i,j) &= \sum_{r=i}^{\lfloor \frac{i+j-1}{2} \rfloor} (-1)^{r-i}\binom{j-r-1}{r-i}x_r,\\
\gamma(1-l,2i+1+l) &= \sum_{r=1-l}^{\lfloor \frac{1-l+2i+1+l-1}{2} \rfloor} (-1)^{r+l-1}\binom{2i+l-r}{r+l-1}x_r\\
&= \sum_{r=1-l}^{\lfloor \frac{1+2i}{2} \rfloor} (-1)^{r+l-1}\binom{2i+l-r}{r+l-1}x_r\\
&= \sum_{r=1-l}^{i} (-1)^{r+l-1}\binom{2i+l-r}{r+l-1}x_r.
\end{aligned}$$

Para $r = 1-l$, temos $\binom{2i+l-1+l}{1-l+l-1}x_{1-l} = \binom{2i-1}{0}x_{1-l} = x_{1-l} = \gamma(1-l,2-l)$.

Para $r = i$, temos $\binom{i+l}{i+l-1}x_i = (-1)^{i+l-1}\dfrac{(i+l)(i+l-1)!}{(i+l-1)!}x_i = (-1)^{i+l-1}(i+l)x_i$.

Logo, $\gamma(1-l,2i+1+l) = x_{1-l} + \sum' + (-1)^{i+l-1}(i+l)x_i$, com $\sum'$ combinação linear de x_r, $2-l < r \leq i-1$.

Vamos calcular $\gamma(1-l,i+1) = \sum_{r=1-l}^{\lfloor \frac{i-l+1}{2} \rfloor} (-1)^{r+l-1}\binom{i-r}{r+l-1}x_r$.

Assim, fazendo $r = 1-l$, temos $\binom{i-(1-l)}{(1-l)+l-1}x_{1-l} = \binom{i+l-1}{0}x_{1-l} = x_{1-l}$.

Logo, $\gamma(1-l,i+1) = x_{1-l} + \sum''$, com $\sum''$ combinação linear de x_r,

$$2-l \leq r \leq \left\lfloor \frac{i-l+1}{2} \right\rfloor \leq \frac{i-l+1}{2}.$$

Se escolhermos $i \geq 2-l$, teremos $\quad i > 1-l \implies 2i > i+1-l \implies i > \dfrac{i+1-l}{2}$.
Então, se $i \geq 2-l$, teremos que $\sum''$ é combinação linear de $2-l \leq r < i$

Como $\gamma(i,i+1)\Big[\gamma(1-l,2i+1+l) - \gamma(1-l,i+1)\Big] = 0$, segue que

$$x_i\Big[x_{1-l} + \sum' + (-1)^{i+l-1}(i+l)x_i - x_{1-l} - \sum''\Big] = x_i\Big[\sum''' + (-1)^{i+l-1}(i+l)x_i\Big] = 0,$$

com $\sum'''$ combinação linear de x_r, $2-l \leq r \leq i-1$.

Vamos mostrar por indução em i que $x_i = 0, \forall\ i = 2-l, 3-l, ..., (p-1)-l$.

Seja $i = 2-l$. Daí, $x_i\Big[\sum''' + (-1)^{i+l-1}(i+l)x_i\Big] = 0$ se reduz a

$x_{2-l}\Big[(-1)(i+l)x_{2-l}\Big] = -2x_{2-l}^2 = 0$ Logo, $x_{2-l} = 0$.

Seja $i > 2-l$. Pela hipótese de indução, $x_{2-l} = \cdots = x_{i-1} = 0$. Consequentemente,

temos que $\sum''' = 0$. Daí, temos $(-1)^{i+l-1}(i+l)x_i^2 = 0$. Como $i + l \not\equiv 0$ (mod p),

$$x_i^2 = 0 \quad \Longrightarrow \quad x_i = 0, \quad \text{para} \quad 2-l \leq i \leq p-1-l.$$

Seja agora $i = 1-l$. Daí, $x_{1-l} = \gamma(1-l, 2-l)$ (pela prop. P_7) $= \gamma(1-l+p-1, 2-l) = \gamma(p-l, 2-l) = -\gamma(2-l, p-l)$.

Ainda, $-\gamma(2-l, p-l) = \displaystyle\sum_{r=2-l}^{p-l-1} (-1)^{r-1+l}\binom{p-l-r-1}{r-2-l}x_r = 0$, como vimos acima, pois $x_r = 0$, para $2-l \leq r \leq p-1-l$. Ou seja, $x_{1-l} = 0$, e $x_i = 0, \forall\ 2-l \leq i \leq p-1-l$. Como γ tem período $p-1$, e munidos das propriedades P_2 e P_3, temos que $x_r = 0, \forall\ r \in \mathbb{Z}$. Desse modo, $\gamma(i, j) = 0$ para quaisquer $i, j \in \mathbb{Z}$. Isso implica que $\alpha \equiv 0$, o que é uma contradição.
Portanto, devemos ter, necessariamente, $l(G) > \dfrac{m-3p+5}{2}$, ou ainda, $l(G) \geq \dfrac{m-3p+6}{2}$.

□

Corolário 3.1.3. *Seja G um p-grupo de classe maximal. Então, se $i \geq \dfrac{3p-7}{3}$, G_i tem classe de nilpotência menor ou igual a* 2

Demonstração. Pelo Teorema 3.1.2, temos $2l \geq m - 3p + 6$, então $\gamma_2(G_i) = [G_i, G_i] = [G_i, G_{i+1}] \leq G_{2i+l+1}$ e $\gamma_3(G_i) = [\gamma_2(G_i), G_i] \leq G_{3i+2l+1}$. Se $3i+2l+1 \geq m$, ou seja, $i \geq (m-2l-1)/3$, então G_i tem classe menor ou igual a 2. Sendo $\dfrac{m-2l-1}{3} \leq \dfrac{m-m+3p-6-1}{3} =$

$= \dfrac{3p-7}{3}$, se $i \geq \dfrac{3p-7}{3}$, temos o resultado. □

Observação 3.1.4. *Se G é um* 11*-grupo, então G_9 tem classe de nilpotência menor ou igual a* 2.

Capítulo 4

Uma melhor limitação inferior para o grau de comutatividade

4.1 Resultados de Fernández-Alcober

Vamos mostrar agora o resultado principal objetivado por esse trabalho, o qual é um teorema que melhora a limitação vista no teorema apresentado acima. Como já foram apresentadas as limitações para os primos 2, 3 e 5 (os quais não obedecem à limitação a seguir), veremos que o resultado vale para todo número primo maior ou igual a 7.

Lema 4.1.1 (Fernández-Alcober)**.** *Se $l(G) \leq m - p - 2$, então podemos estender a função α a uma função β, que cumpre as propriedades P_3, P_4 e P_7 de α e tem domínio $\mathbb{N}^2$.*

Demonstração. Para $j \geq 1$, seja $\beta(1, j) = \alpha(1, j_0)$, $j_0 \in [1, p-1]$ e $j \equiv j_0 \bmod (p-1)$. Pela propriedade P_7 de α, temos que $\beta(1, j) = \alpha(1, j)$, para $1 \leq j \leq m - l - 2$. Agora vamos definir $\beta(i, j)$ para todo $i, j \geq 1$ de forma indutiva sobre i, através de $\beta(i, j) = \beta(i-1, j) - \beta(i-1, j+1)$. Baseados nessa relação, podemos mostrar por indução em r que

$$\beta(i, j) = \sum_{k=0}^{r} (-1)^k \binom{r}{k} \beta(i - r, j + k), \text{ para } i \geq r + 1 \qquad \text{(I)}$$

e

$$\beta(i, j) = \sum_{k=0}^{r} (-1)^k \binom{r}{k} \beta(i + k, j - r), \text{ para } j \geq r + 1. \qquad \text{(II)}$$

Pela propriedade P_4, podemos deduzir a fórmula semelhante para α, com a restrição necessária $i + j \leq m - l - 1$. Tomando $r = i - 1$ em (I), temos

$$\begin{aligned}\beta(i,j) &= \sum_{k=0}^{i-1}(-1)^k\binom{i-1}{k}\beta(1,j+k)\\ &= \sum_{k=0}^{i-1}(-1)^k\binom{i-1}{k}\alpha(1,j+k)\\ &= \alpha(i,j)\end{aligned}$$

para $i+j \leq m-l-1$. Dessa forma, temos que β é uma extensão de α. Agora devemos verificar que β satisfaz, de fato, as propriedades P_3, P_4 e P_7 de α. Pela própria definição de β, temos que a propriedade P_4 é automaticamente satisfeita. Para mostrar P_7, façamos indução sobre $i \geq 1$:

Para $i = 1$, temos que $\beta(1, j+p-1) = \beta(1, j)$, pela definição de $\beta(1, j)$. Se $i \geq 2$, então, por P_4,

$$\begin{aligned}\beta(i,j) &= \beta(i-1,j) - \beta(i-1,j+1)\\ &= \beta(i-1,j+p-1) - \beta(i-1,j+p)\\ &= \beta(i,j+p-1).\end{aligned}$$

Por outro lado, fazendo $r = p$ em (I),

$$\begin{aligned}\beta(i+p-1,j) &= \sum_{k=0}^{p}(-1)^k\binom{p}{k}\beta(i-1,j+k)\\ &= \beta(i-1,j) - \beta(i-1,j+p)\\ &= \beta(i-1,j) - \beta(i-1,j+1)\\ &= \beta(i,j)\end{aligned}$$

Vamos mostrar agora a validade da propriedade P_3 para β, isto é, $\beta(i,j) = -\beta(j,i)$, para todo $i, j \geq 1$. Mostremos o resultado por indução em $i+j$. Se $i+j \leq m-l-1$, então β coincide com α, e vale o resultado. Para $i+j \geq m-l$ ($\geq p+2$), então

$$\begin{aligned}
\beta(i,j) &= \sum_{k=0}^{i-1}(-1)^k\binom{i-1}{k}\beta(1,j+k)\\
&= \sum_{k=0}^{i-2}(-1)^k\binom{i-1}{k}\beta(1,j+k)+(-1)^{i-1}\beta(1,j+i-1)
\end{aligned}$$

(Como $j+k+1 \leq j+i-2+1 \leq j+i-1$, estamos na hipótese de indução)

$$\begin{aligned}
&= -\sum_{k=0}^{i-2}(-1)^k\binom{i-1}{k}\beta(j+k,1)+(-1)^{i-1}\beta(1,j+i-1)\\
&= -\sum_{k=0}^{i-2}(-1)^k\binom{i-1}{k}\beta(j+k,1)+(-1)^{i-1}\beta(1,j+i-p)
\end{aligned}$$

(Como $1+j+1-p < i+j \leq j+i-1$, novamente, estamos na hipótese de indução)

$$\begin{aligned}
&= -\left[\sum_{k=0}^{i-2}(-1)^k\binom{i-1}{k}\beta(j+k,1)+(-1)^{i-1}\beta(j+i-p,1)\right]\\
&= -\sum_{k=0}^{i-1}(-1)^k\binom{i-1}{k}\beta(j+k,1)\\
&= -\beta(j,i).
\end{aligned}$$

□

Lema 4.1.2 (Fernández-Alcober)**.** *Se $l(G) \leq m-p-2$, então podemos estender a função β do Lema 4.1.1 a uma função γ, que cumpre as mesmas propriedades que β, e tem domínio $\mathbb{Z}^2$.*

Demonstração. Se $i, j \in \mathbb{Z}$, tomemos $i_0, j_0 \in [1, p-1]$, tais que $i \equiv i_0 \pmod{p-1}$ e $j \equiv j_0 \pmod{p-1}$. Definamos $\gamma(i,j) = \beta(i_0, j_0)$, onde β é a função obtida no lema anterior. Dessa forma, claramente γ é uma extensão de β (e também de α). Logo, pela definição, γ cumpre as propriedades P_3, P_4 e P_7. □

Observação 4.1.3. *No lema acima, são citadas apenas as propriedades P_3, P_4 e P_7, porém a função γ verifica também as propriedades P_1, P_2 e P_5.*

Lema 4.1.4. *[Fernández-Alcober] Seja $p \geq 7$. Se $l(G) \leq \dfrac{m-2p+4}{2}$ e γ é a função obtida no Lema 4.1.2, então*

$\Gamma_\gamma(i,j,k) = \gamma(i,j)\gamma(i+j+l,k)+\gamma(j,k)\gamma(j+k+l,i)+\gamma(k,i)\gamma(k+i+l,j) = 0,$
para todo $i, j, k \in \mathbb{Z}$.

Demonstração. Inicialmente, notemos que faz sentido usarmos a função γ, pois $l \leq \dfrac{m-2p+4}{2}$ e $p \geq 7$ implicam em $l \leq m-p-2$. De fato, pois, como $l(G) \geq 0$ sempre, temos que $l \leq 2l \leq m-2p+4 \leq m-p-p+4 \leq m-p-7+4 \leq m-p-3 \leq m-p-2$.

Tal como no Lema 3.1.1, temos que, se tivermos dois dos valores i, j, k iguais, obviamente $\Gamma_\gamma(i,j,k) = 0$, pela propriedade P_2. Além disso, também claramente, Γ_γ é periódica nas três variáveis, de período $p-1$. Vamos mostrar o resultado em três etapas.

Inicialmente, mostremos que $\Gamma_\gamma(1,j,k) = 0$, para $j,k \geq 1$ e $j+k \leq 2p-6$. Temos o resultado de imediato, pois
$2l \leq m-2p+4 \Longrightarrow m-2l \geq 2p-4 \Longrightarrow m-2l-1 \geq 2p-5 \geq 1+j+k$, o que implica

$$\Gamma_\gamma(1,j,k) = \alpha(1,j)\alpha(1+j+l,k) + \alpha(j,k)\alpha(j+k+l,1) + \alpha(k,1)\alpha(k+1+l,j) = 0.$$

Agora, mostremos que $\Gamma_\gamma(1,j,k) = 0$, para $1 \leq j,k \leq p-1$. Como $\Gamma_\gamma(1,j,j) = 0$ e $\Gamma_\gamma(1,j,k) = -\Gamma_\gamma(1,k,j)$, basta considerar $\Gamma_\gamma(1,p-2,p-1)$, $\Gamma_\gamma(1,p-3,p-1)$, $\Gamma_\gamma(1,p-4,p-1)$ e $\Gamma_\gamma(1,p-3,p-2)$.
De fato, pois, se $k = p-1$, temos $\Gamma_\gamma(1,j,p-1)$, $1 \leq j \leq p-1$. Notemos que, se $j+p-1 \leq 2p-6$, já temos válido o resultado. Observemos que $j+p-1 > 2p-6 \Longrightarrow j > p-5$. Portanto, basta considerarmos $p-5 < j < p-1$, uma vez que $\Gamma_\gamma(1,p-1,p-1) = 0$.

No caso de $k = p-2$, temos $\Gamma_\gamma(1,j,p-2)$. Assim, devemos ter $j+p-2 > 2p-6$, como observado anteriormente. Com isso, $j > p-4$. Daí, $p-4 < j < p-2$, ou seja, basta considerarmos $j = p-3$, pois, $\Gamma_\gamma(1,p-2,p-2) = 0$, e $\Gamma_\gamma(1,p-1,p-2) = -\Gamma_\gamma(1,p-2,p-1)$.

Finalmente, se $k = p-3$, devemos ter $j > p-3$, ou seja, teremos $\Gamma_\gamma(1,p-2,p-3) = -\Gamma_\gamma(1,p-3,p-2)$.

Dando continuidade, pela propriedade P_4 para γ, temos que

$$\Gamma_\gamma(r,j,k) = \Gamma_\gamma(r+1,j,k) + \Gamma_\gamma(r,j+1,k) + \Gamma_\gamma(r,j,k+1).$$

Suponhamos que $i < j$. Variando r de i até $j-1$ na igualdade acima, temos

$$\sum_{r=i}^{j-1} \Gamma_\gamma(r,j,k) = \sum_{r=i}^{j-1} \Gamma_\gamma(r+1,j,k) + \sum_{r=i}^{j-1} \Gamma_\gamma(r,j+1,k) + \sum_{r=i}^{j-1} \Gamma_\gamma(r,j,k+1)$$

$$\Longrightarrow \Gamma_\gamma(i,j,k) + \sum_{r=i+1}^{j-1} \Gamma_\gamma(r,j,k) = \sum_{r=i+1}^{j} \Gamma_\gamma(r,j,k) + \sum_{r=i}^{j-1} \Gamma_\gamma(r,j+1,k) + \sum_{r=i}^{j-1} \Gamma_\gamma(r,j,k+1)$$

$$\Longrightarrow \Gamma_\gamma(i,j,k) + \sum_{r=i+1}^{j-1} \Gamma_\gamma(r,j,k) = \Gamma_\gamma(j,j,k) + \sum_{r=i+1}^{j-1} \Gamma_\gamma(r,j,k) + \sum_{r=i}^{j-1} \Gamma_\gamma(r,j+1,k) + \sum_{r=i}^{j-1} \Gamma_\gamma(r,j,k+1)$$

$$\Longrightarrow \Gamma_\gamma(i,j,k) = \sum_{r=i}^{j-1} \Gamma_\gamma(r,j+1,k) + \sum_{r=i}^{j-1} \Gamma_\gamma(r,j,k+1), \text{ já que } \Gamma_\gamma(j,j,k) = 0.$$

Aplicando essa fórmula anterior a $(i, p-2, p-1)$, obtemos

$$\begin{aligned}
\Gamma_\gamma(i,p-2,p-1) &= \sum_{r=i}^{p-3} \Gamma_\gamma(r,p-1,p-1) + \sum_{r=i}^{p-3} \Gamma_\gamma(r,p-2,p) \\
(\text{ pela periodicidade }) &= \sum_{r=i}^{p-3} \Gamma_\gamma(1,r,p-2) \\
(\text{ para } j+k \leq 2p-6, \Gamma_\gamma(1,j,k) = 0\ ) &= \Gamma_\gamma(1,p-3,p-2), \text{ para } 1 \leq i \leq p-3. \qquad \text{(III)}
\end{aligned}$$

Ainda, se $1 \leq i \leq p-4$, então

$$\begin{aligned}
\Gamma_\gamma(i,p-3,p-1) &= \sum_{r=i}^{p-4} \Gamma_\gamma(r,p-2,p-1) + \sum_{r=i}^{p-4} \Gamma_\gamma(r,p-3,p) \\
(\text{ pelo resultado anterior }) &= (p-3-i)\Gamma_\gamma(1,p-3,p-2) + \sum_{r=i}^{p-4} \Gamma_\gamma(1,r,p-3) \\
(\ \Gamma_\gamma(1,j,p-3) = 0, \text{ para } j \leq p-4\ ) &= (p-3-i)\Gamma_\gamma(1,p-3,p-2). \qquad \text{(IV)}
\end{aligned}$$

Por outro lado,

$$\begin{aligned}
\Gamma_\gamma(1,p-3,p-2) &= \sum_{r=i}^{p-4} \Gamma_\gamma(r,p-2,p-2) + \sum_{r=i}^{p-4} \Gamma_\gamma(r,p-3,p-1) \\
(\text{ pelo resultado anterior }) &= \sum_{r=1}^{p-4} (p-3-r)\Gamma_\gamma(1,p-3,p-2) \\
* &= \binom{p-3}{2}\Gamma_\gamma(1,p-3,p-2) \\
\Gamma_\gamma(1,p-3,p-2) &= 6\,\Gamma_\gamma(1,p-3,p-2) \\
&\Longrightarrow 5\,\Gamma_\gamma(1,p-3,p-2) = 0
\end{aligned}$$

* Observemos que $\binom{p-3}{2} = \dfrac{(p-3)(p-4)}{2} \equiv \dfrac{(-3)(-4)}{2} \pmod{p}$.

Como $p \geq 7$, segue que $\Gamma_\gamma(1,p-3,p-2) = 0$. Então (III) e (IV) também são iguais a zero. Daí, resta apenas mostrar que $\Gamma_\gamma(1,p-4,p-1) = 0$, o que segue de

$$\Gamma_\gamma(1, p-4, p-1) = \sum_{r=1}^{p-5} \Gamma_\gamma(r, p-3, p-1) + \sum_{r=1}^{p-5} \Gamma_\gamma(1, r, p-4).$$

Onde a primeira parcela é igual a 0 por (IV), e a segunda, pelo motivo de que $j + k \leq 2p - 6$.

Finalmente, mostremos que $\Gamma_\gamma(i, j, k) = 0$, para todo $i, j, k \in \mathbb{Z}$. Primeiro vamos provar para $i \geq 1$, por indução. Suponhamos que $i = 1$. Se $j \equiv j_0 \pmod{p-1}$ e $k \equiv k_0 \pmod{p-1}$, com $1 \leq j_0 \leq p-1$ e $1 \leq k_0 \leq p-1$, então $\Gamma_\gamma(1, j, k) = \Gamma_\gamma(1, j_0, k_0) = 0$ segue pela parte anterior. Se $i \geq 2$, a indução fica completa pela seguinte relação:

$$\Gamma_\gamma(i, j, k) = \Gamma_\gamma(i-1, j, k) - \Gamma_\gamma(i-1, j+1, k) - \Gamma_\gamma(i-1, j, k+1).$$

Se $i \leq 0$, é suficiente tomar $t \geq 1$, tal que $t \equiv i \pmod{p-1}$, e notemos que $\Gamma_\gamma(i, j, k) = \Gamma_\gamma(t, j, k) = 0$.

□

Teorema 4.1.5 (Fernández-Alcober)**.** *Seja $p \geq 7$ um número primo. Se G é um p-grupo de classe maximal de ordem p^m, então $l(G) \geq \dfrac{m - 2p + 5}{2}$.*

Demonstração. Suponhamos, por absurdo, que $l(G) \leq \dfrac{m - 2p + 4}{2}$. Pelo Lema 4.1.4,

$$\begin{aligned}
0 &= \Gamma_\gamma(j+1, j, 1-l) \\
&= \gamma(j+1, j)\gamma(j+1+j+l, 1-l) + \gamma(j, 1-l)\gamma(j+1-l+l, j+1) + \\
&+ \gamma(1-l, j+1)\gamma(1-l+j+1+l, j) \\
&= \gamma(j+1, j)\gamma(2j+l+1, 1-l) + \gamma(j, 1-l)\gamma(j+1, j+1) + \\
&+ \gamma(1-l, j+1)\gamma(j+2, j) \\
&= \gamma(j+1, j)\gamma(2j+l+1, 1-l) + \gamma(1-l, j+1)\gamma(j+1, j) \\
&= \gamma(j+1, j)\Big[\gamma(2j+l+1, 1-l) + \gamma(1-l, j+1)\Big] \\
&= \gamma(j+1, j)\Big[\gamma(2j+l+1, 1-l) - \gamma(j+1, 1-l)\Big], \qquad (V)
\end{aligned}$$

para todo $j \in \mathbb{Z}$. Por outro lado, denotando $x_i = \gamma(i+1, i)$, temos que

$$\gamma(i+k, i) = \sum_{r=0}^{\lfloor \frac{k-1}{2} \rfloor} (-1)^r \binom{k-r-1}{r} x_{i+r}. \qquad (VI)$$

De fato pois, por indução em $k \geq 1$, temos:

Se $k = 1$, $\gamma(i+1,i) = \sum_{r=0}^{\lfloor \frac{1-1}{2} \rfloor} (-1)^r \binom{1-r-1}{r} x_{i+r} = \binom{0}{0} x_i = \gamma(i+1,i)$.

Supondo o resultado válido até $k-1$, vale

$$\gamma(i+k-1,i) = \sum_{r=0}^{\lfloor \frac{k-2}{2} \rfloor} (-1)^r \binom{k-r-2}{r} x_{i+r}.$$

Daí,
Pela propriedade P_4, $\gamma(i+k-1,i) = \gamma(i+k,i) + \gamma(i+k-1,i+1)$

$$\begin{aligned}
\gamma(i+k,i) &= \gamma(i+k-1,i) - \gamma(i+k-1,i+1) \\
&= \gamma(i+k-1,i) - \gamma((i+1)+(k-2),i+1) \\
&= \sum_{r=0}^{\lfloor \frac{k-2}{2} \rfloor} (-1)^r \binom{k-r-2}{r} x_{i+r} - \sum_{r=0}^{\lfloor \frac{k-3}{2} \rfloor} (-1)^r \binom{k-r-3}{r} x_{i+1+r} \\
&= \sum_{r=0}^{\lfloor \frac{k-2}{2} \rfloor} (-1)^r \binom{k-r-2}{r} x_{i+r} + \sum_{r=1}^{\lfloor \frac{k-3}{2} \rfloor+1} (-1)^r \binom{k-r-2}{r-1} x_{i+r}
\end{aligned}$$

(No 2º somatório, o termo obtido para $r = 0$ vale 0)

$$\begin{aligned}
&= \sum_{r=0}^{\lfloor \frac{k-2}{2} \rfloor} (-1)^r \binom{k-r-2}{r} x_{i+r} + \sum_{r=0}^{\lfloor \frac{k-3}{2} \rfloor+1} (-1)^r \binom{k-r-2}{r-1} x_{i+r}
\end{aligned}$$

(No 1º somatório, o termo obtido para $r = \left\lfloor \frac{k-3}{2} \right\rfloor + 1$ vale 0)

$$\begin{aligned}
&= \sum_{r=0}^{\lfloor \frac{k-3}{2} \rfloor+1} (-1)^r \binom{k-r-2}{r} x_{i+r} + \sum_{r=0}^{\lfloor \frac{k-3}{2} \rfloor+1} (-1)^r \binom{k-r-2}{r-1} x_{i+r}
\end{aligned}$$

(soma de coeficientes binomiais)

$$\begin{aligned}
&= \sum_{r=0}^{\lfloor \frac{k-3}{2} \rfloor+1} (-1)^r \binom{k-r-1}{r} x_{i+r}
\end{aligned}$$

$$= \sum_{r=0}^{\left\lfloor \frac{k-1}{2} \right\rfloor} (-1)^r \binom{k-r-1}{r} x_{i+r}$$

Aplicando a fórmula anterior a (V), para $j \geq 2-l$, temos

$$\gamma(2j+l+1, 1-l) = \sum_{r=0}^{\left\lfloor \frac{2j+2l-1}{2} \right\rfloor = j+l-1} (-1)^r \binom{k-r-1}{r} x_{1-l+r}.$$

Para $r = 0$, temos x_{1-l}.

Para $r = j+l-1$, temos $(-1)^{j+l-1}\binom{2j+2l-j-l+1-1}{j+l-1} x_{1-l+j+l-1}$

$= (-1)^{j+l-1}(j+l)x_j$. Logo, $\gamma(2j+l+1, 1-l) = x_{1-l} + \sum' + (-1)^{j+l-1}(j+l)x_j$, com $\sum'$ combinação linear de x_i, com $2-l \leq i \leq j-1$.

Por outro lado, temos que $\gamma(j+1, 1-l) = \sum_{r=0}^{\left\lfloor \frac{j+l-1}{2} \right\rfloor} (-1)^r \binom{k-r-1}{r} x_{1-l+r}$.

Daí, fazendo $r = 0$, temos x_{1-l}.

Logo, $\gamma(j+1, 1-l) = x_{1-l} + \sum''$, onde $\sum''$ é combinação linear de x_i, com $i \geq 2-l$.

A fim de juntarmos as combinações $\sum'$ e $\sum''$ sem que apareça o termo x_j em $\sum''$ (que aparece no termo visto anteriormente), devemos ter $i < j$.

Assim, $i = 1-l+r < j \iff 1-l+\left\lfloor \frac{j+l-1}{2} \right\rfloor < j$.

Notemos que $1-l+\left\lfloor \frac{j+l-1}{2} \right\rfloor \leq 1-l+\frac{j+l-1}{2}$. Logo,

$\frac{2-2l+j+l-1}{2} < j \iff -l+j+1 < 2j \iff j > 1-l \iff j \geq 2-l$.

Desse forma, se tivermos $j \geq 2-l$, temos que $i < j$.

Portanto, $\sum''$ é combinação linear de x_i, com $2-l \leq i \leq j-1$.

Daí,

$\gamma(j+1, j)\Big[\gamma(2j+l+1, 1-l) - \gamma(j+1, 1-l)\Big] =$

$$= x_j\Big[x_{1-l} + \sum{}' + (-1)^{j+l-1}(j+l)x_j - x_{1-l} - \sum{}''\Big]$$

$$= x_j\Big[(-1)^{j+l-1}(j+l)x_j + \sum{}'''\Big] = 0, \text{ com } \sum{}''' \text{ comb. linear de } x_{2-l}, \cdots, x_{j-1}. \qquad \text{(VII)}$$

Como $j + l \not\equiv 0 \pmod{p}$, para $j = 2 - l, \cdots, p - 1 - l$, substituindo esses valores de j em (VII), concluímos que $x_{2-l} = \cdots = x_{p-1-l} = 0$, pois:

Seja $j = 2 - l$. Daí teremos $x_{2-l}\Big[(-1)^1(2)x_{2-l} + 0\Big] = 0$. Logo, $x_{2-l} = 0$.

Para $j = 3 - l$, $x_{3-l}\Big[(-1)^2(3)x_{3-l} + \sum{}'''\Big] = 0$, onde $\sum{}'''$ só possui o termo x_{2-l}.

Prosseguindo desse modo, concluímos que $x_j = 0$, para $2 - l \leq j \leq p - 1 - l$.

Ademais, $x_{1-l} = \gamma(2 - l, 1 - l) = -\gamma(p - l, 2 - l) = 0$, pois, por (VI), $\gamma(p - l, 2 - l)$ é combinação linear de $x_{2-l}, \cdots, x_{p-l-1}$.

Finalmente, pela periodicidade de γ (propriedade P_7), temos que $x_i = 0$, para todo $i \in \mathbb{Z}$. Dessa forma, a fórmula (VI) implica que $\gamma(i, j) = 0$, para quaisquer $i, j \in \mathbb{Z}$. Sendo assim, temos que $\alpha \equiv 0$, o que é uma contradição.

Portanto, devemos ter, necessariamente, $l(G) \geq \dfrac{m - 2p + 5}{2}$.

□

4.2 Consequências do Teorema de Fernández-Alcober

Com o resultado do Teorema de Fernández-Alcober, temos alguns corolários que nos fornecem informações a respeito de um p-grupo G ou de alguns subgrupos, em relação à classe de nilpotência e ao comprimento derivado, de acordo com sua ordem.

Corolário 4.2.1. *Em qualquer p-grupo de classe maximal, G_i tem classe de nilpotência ≤ 2, onde i é o menor inteiro positivo que é maior ou igual a $\dfrac{2p - 6}{3}$.*

Demonstração. Seja $3i \geq 2p-6$. Logo, $2p \leq 3i+6$. Pelo Teorema 4.1.5, $2l(G) \geq m-2p+5 \Longrightarrow 2l \geq m - 3i - 6 + 5 \Longrightarrow m \leq 2l + 3i + 1$. Observemos que $\gamma_2(G_i) = [G_i, G_i] = [G_i, G_{i+1}] \leq G_{2i+l+1}$. Daí, $\gamma_3(G_i) \leq [G_{2i+l+1}, G_i] \leq G_{3i+2l+1} \leq G_m = \{1\}$, pois $2l + 3i + 1 \geq m$.

□

Observação 4.2.2. *O Corolário 4.2.1 nos fornece que, para $p = 11$, G_6 tem classe de nilpotência ≤ 2, enquanto no Corolário 3.1.2, obtido por Leedham-Green e McKay, tínhamos que G_9 tinha classe de nilpotência ≤ 2.*

Corolário 4.2.3. *Se $m \geq 6p - 25$, então G_1 tem classe de nilpotência, no máximo, 3.*

Demonstração. Pelo Teorema 4.1.5 (Fernández-Alcober), temos que $2l(G) \geq m-2p+5$, ou seja, $m \leq 2l+2p-5$. Por outro lado, pela hipótese do corolário, devemos ter $m \geq 6p-25$. Logo, temos $6p-25 \leq m \leq 2l+2p-5 \Longrightarrow 6p-25 \leq 2l+2p-5 \Longrightarrow 4p \leq 2l+20 \Longrightarrow 2p \leq l+10$. Sendo assim, $m \leq 2l + 2p - 5 \Longrightarrow m \leq 2l + l + 10 - 5 \Longrightarrow m \leq 3l + 5$. Vamos calcular agora $\gamma_4(G_1)$. Assim,
$\gamma_4(G_1) = [G_1, G_1, G_1, G_1] = [G_1, G_2, G_1, G_1] \leq [G_{3+l}, G_1, G_1] \leq [G_{4+2l}, G_1] \leq G_{5+3l} \leq G_m =$
$= \{1\}$, pois $3l + 5 \geq m$.

□

Corolário 4.2.4. *Se $m \geq 6p - 37$, então o comprimento derivado de G é, no máximo, 3.*

Demonstração. Novamente, pelo Teorema 4.1.5, temos que $2l(G) \geq m - 2p + 5$, ou seja, $m \leq 2l+2p-5$. Por outro lado, pela hipótese do corolário, devemos ter $m \geq 6p-37$. Logo, temos $6p - 37 \leq m \leq 2l + 2p - 5 \Longrightarrow 6p - 37 \leq 2l + 2p - 5 \Longrightarrow 4p \leq 2l + 32 \Longrightarrow 2p \leq l + 16$. Sendo assim, $m \leq 2l + 2p - 5 \Longrightarrow m \leq 2l + l + 16 - 5 \Longrightarrow m \leq 3l + 11$.
Temos $G' = G_2 = [G, G]$. Assim, $G'' = [G', G'] = [G_2, G_2] = [G_2, G_3] \leq G_{5+l}$.
Logo, $G''' = [G'', G''] \leq [G_{5+l}, G_{5+l}] = [G_{5+l}, G_{6+l}] \leq G_{11+3l} \leq G_m = \{1\}$, pois $3l + 11 \geq m$.

□

Corolário 4.2.5. *Para $p \geq 3$, o comprimento derivado de qualquer p-grupo de classe maximal é, no máximo, $[log_2(p-1)] + 1$.*

Demonstração. Para $p = 3$, lembremos que o comprimento derivado de $G \leq 2$, pelo Teorema 2.3.3, e $[\log_2(p-1)] + 1 = 2$.

Como observado no Corolário 4.2.4, $G'' \leq G_{5+l}$ e $G''' \leq G_{11+3l}$. Em geral, $G^{(i)} \leq G_t$, onde $t = 3 \cdot 2^{i-1} + l \cdot (2^{i-1} - 1) - 1$. Seja d o comprimento derivado de G. Daí, $G^{d-1} \neq 1$, e, então, $3 \cdot 2^{d-2} + l \cdot (2^{d-2} - 1) - 1 < m$.
Se $l(G) = 0$, pelo Teorema de Blackburn, temos que $m \leq p+1$ e, portanto, $3 \cdot 2^{d-2} - 1 < p+1$. Daí, $3 \cdot 2^{d-2} \leq p + 1 \Longrightarrow 2^{d-2} \leq (p+1)/3 \Longrightarrow 2^{d-1} \leq (p+1) \cdot 2/3 \leq p - 1$, se $p \geq 5$. Logo, $d - 1 \leq \log_2 p - 1$.

Seja $l(G) \geq 1$. Temos $3 \cdot 2^{d-2} + l \cdot (2^{d-2} - 1) - 1 < m$. Daí,

$$\begin{aligned}
3 \cdot 2^{d-2} + l \cdot 2^{d-2} - l - 1 &< m \\
(3 + l) \cdot 2^{d-2} - l - 1 &< 2l + 2p - 5 \\
2^{d-2} &< \frac{3l + 2p - 4}{3 + l} \\
&= \frac{9 + 3l + 2p - 4 - 9}{3 + l} \\
&= 3 + \frac{2p - 13}{3 + l} \\
(\text{ pois } l(G) \geq 1\ ) &\leq 3 + \frac{2p - 13}{4} \\
\Longrightarrow 2^{d-2} &< \frac{(2p - 1)}{4}
\end{aligned}$$

Assim, $2^d < 2p - 1 \Longrightarrow 2^d \leq 2p - 2 \Longrightarrow 2^{d-1} \leq p - 1 \Longrightarrow d - 1 \leq \log_2(p - 1)$.

□

Conclusão

Este trabalho teve como objetivo principal mostrar um resultado acerca da limitação inferior para o grau de comutatividade de um p-grupo finito de classe maximal. Apresentamos o Teorema de Fernández-Alcober, que nos dá uma limitação inferior para o grau de comutatividade de um p-grupo finito de classe maximal, melhorando a limitação provada por Leedham-Green e McKay. De acordo com o grau de comutatividade, podemos obter informações sobre p-grupos, que possuem uma estrutura difícil de ser estudada. Esse estudo é de grande relevância, pois ainda não foram classificados todos os p-grupos finitos. Através de informações a respeito do grau de comutatividade de um p-grupo G, podemos conhecer sua estrutura, e nos possibilita determinar, por exemplo, uma classe de grupos isomorfos, à qual tal grupo pertence.

Bibliografia

[1] Blackburn, N. *On a special class of p-groups*, Acta Math, **100** (1958), 45–92.

[2] Fernández-Alcober, G. A. *An introduction to finite p-groups: regular p-groups and groups of maximal class*. Notas de curso - Escola de Álgebra, Brasília, julho de 2000.

[3] Fernández-Alcober, G. A. *The exact lower bound for degree of commutativity of a p-group of maximal class*, J. Algebra, **174** (1995), Volume 256, Issue 2, 375–401.

[4] Leedham-Green, C. R.; Mckay, S. *On p-groups of maximal class*, II, Quart. J. Math. Oxford Ser. (2) **29** (1978), 175–186.

[5] Robinson, D. J. S. *A course in the theory of groups* – 2nd ed. Springer (1995).